

Your Body, Our Data: Unfair and Unsafe Privacy Practices of Popular Fertility Apps

Katharine Kemp
March 2023



UNSW
SYDNEY



UNSW
Allens Hub
for technology, law & innovation



Contents

02	Acknowledgements
03	Background
04	Consumer Attitudes to Data Practices
05	Sensitivity of Data Collected
13	'We Never Sell Your Data' – Until We Do
15	Confusing and Misleading Privacy Choices
18	'Research' Uses Without Ethics Oversight or Reliable De-identification
22	Pervasive Tracking and Profiling
25	Unsafe Retention of Consumers' Data
27	Concluding Remarks



Acknowledgements

The research for this project was generously funded by a grant from the UNSW Allens Hub for Technology Law & Innovation. I am also grateful for the insightful comments and suggestions on earlier versions provided by Anna Johnston, Vanessa Teague, Kate Bower and Chandni Gupta, to Linda Fang for research assistance, to Deborah Bordeos for cover design and kind assistance from Amy Gardner. All errors are my own.

About the author

Dr Katharine Kemp is a Senior Lecturer in the Faculty of Law & Justice, UNSW Sydney, and Co-Lead of the “Data as a Source of Market Power” Research Stream for the UNSW Allens Hub for Technology Law & Innovation.

Background

The information collected by fertility apps extends to the innermost workings of a person, from when and how they have sex, whether they had an orgasm and whether they used contraception, when they feel happy, anxious, energetic, sad or panicked, when they bleed and when they don't, how their cervical fluid changes, the medications they take, their changing sleeping patterns, whether they become pregnant, the timing and frequency of contractions in pregnancy, whether they suffer a miscarriage, and what illnesses and disorders afflict them, from constipation and depression to uterine fibroids, polycystic ovary syndrome and infertility.

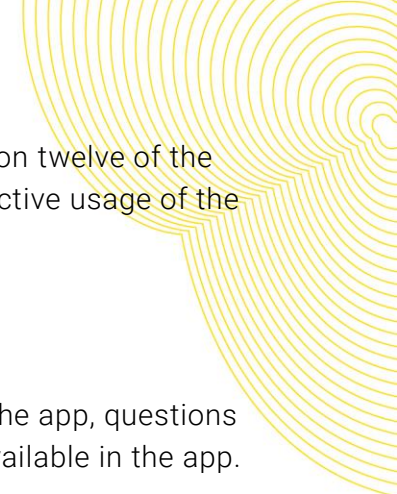
Consumers using these apps may be unaware that many have been strongly criticised for their privacy and security flaws.¹ Operators of some of the most popular apps – including “Flo” and “Glow” – have been sued in the United States for alleged privacy infringements.² Notwithstanding these earlier criticisms and enforcement actions, our analysis reveals numerous unfair and unsafe data practices in some of the most popular fertility apps currently used by Australians. These findings underscore the need for urgent reform of Australian privacy laws, presently under consideration by the Attorney General following the Privacy Act Review by the Attorney General’s Department (‘Privacy Act Review’).³ Some cases also warrant scrutiny under the Australian Consumer Law.

Apps used on mobile phones to track menstrual cycles, sexual activities, opportunities for conceiving a child and symptoms and stages of pregnancy, are seen by industry as part of the broader “FemTech” market which is projected to be worth over US\$50 billion by 2025.⁴ Companies marketing apps that assist consumers in managing these aspects of their fertility, tend to offer apps that meet two or three of the following purposes:

- tracking their menstrual cycle, sometimes to assist in avoiding pregnancy if they are sexually active,⁵ and/or to record symptoms towards menopause;
- trying to conceive a child by tracking their sexual activity, menstrual cycle and other symptoms to identify a “fertile window” for conception; and
- tracking and managing their pregnancy through various stages, including preparations for labour, birth and parenting.

I refer to these as “fertility apps”. The consumer is intended to transition through different “modes” of the one app – for example, from “Period tracking” to “Trying to conceive” to “Pregnancy” mode and back – or through different apps serving these purposes under the one brand, with the consumer directed to download the next app or use the next mode according to their changing needs in managing their fertility.

This study focuses on the data privacy terms, messaging and settings of these services. To the extent that these apps are used to help consumers manage their fertility to either avoid pregnancy or conceive a child, the effectiveness of some has been questioned in previous women’s health studies.⁶ These aspects of the apps are not within the scope of this research but are separately relevant to the trustworthiness of the services offered and whether the benefits of using the app are worth the risks posed to the consumer’s privacy.



To ensure the relevance of the research for consumers, this analysis focuses on twelve of the most popular fertility apps, as indicated by a combination of downloads and active usage of the app in Australia. We conducted a systematic analysis of:

- the currently available privacy policies of each app;
- additional privacy messaging on the app developer's website; and
- the user interface of the app itself, including the steps required to use the app, questions asked of the consumer through the app, and privacy settings (if any) available in the app.

The methodology is explained further in the Appendix. The factors considered as part of this analysis were informed by issues under consideration in the Privacy Act Review and known consumer concerns regarding personal data practices revealed by several surveys from recent years, as explained in the following section.

Consumer attitudes to data practices

Most Australian consumers do not want their online or offline activities tracked and analysed, passed on to other firms, and used for various purposes unconnected with the product or service they sought from the supplier. The 2020 Consumer Policy Research Centre (CPRC) survey showed that the majority of consumers:

- agreed that companies should give them options to opt out of certain types of information collection, use and sharing – 95%;
- agreed that companies should only collect information currently needed for their product or service – 92%;
- find it unacceptable for companies to monitor their online behaviour to show them relevant advertisements and offers – 60%;
- consider it unfair for a company to use personal information to make predictions about the consumer – 76%;
- consider it unfair for a company to collect information about the consumer from other companies – 83%; and
- disagreed that, if they trust a company, they don't mind if the company buys information about them from database companies without asking the consumer – 81%.⁷

According to the 2020 Community Attitudes to Privacy Survey conducted by the Office of the Australian Information Commissioner (OAIC), most Australians are uncomfortable with:

- businesses sharing their personal information with other organisations – 72%; and
- online businesses keeping databases on what they have said and done online – 62%.⁸

The Australian Competition and Consumer Commission (ACCC) 2018 survey indicated that most consumers surveyed considered it to be a misuse of their personal information if digital platforms:

- collect information about the consumer in ways the consumer would not expect – 83%;

- add to information about them with information gathered from other companies the consumer has dealt with – 81%.⁹

In the same survey, most consumers did *not* agree that they did not mind digital platforms collecting more information if the consumer would be more likely to be interested in the ads they receive (62%).¹⁰

In short, most consumers want organisations to: minimise the data collected about them; refrain from seeking further data from third parties or tracking the consumer's behaviour online; use the data for strictly limited purposes; and give the consumer options about the collection, use and disclosure of their personal information.

Sensitivity of data collected

Types of data and methods of collection

This analysis of fertility apps' privacy terms and interfaces revealed certain types of data commonly collected by the apps, and certain common methods of data collection. These types of data and methods of collection, along with examples drawn from various apps in this study, are set out in Table 1. Collection does not always involve the consumer knowingly or actively providing any information. For some of these categories, the consumer is likely to be completely unaware that the data about them is being collected and recorded.

Intimate logging data

Data collection is most obvious to the consumer when they are logging their own symptoms, activities, or test results. The consumer actively enters details about whether they have their period or cramps or changes in cervical fluid, when they had sex and how, whether they used a condom or withdrawal method when they had sex, what type of medication they took and when, or whether they had a positive or negative pregnancy test.

This information can reveal consumers at particularly vulnerable moments in their lives. It may show a couple using the app's "trying to conceive" mode for years on end, while the pregnancy tests return negative results. It can reveal a teenager whose regular periods suddenly stop; a 50-year-old bleeding for weeks at a time; or a mother-of-two in another time zone having protected sex on three days followed by a morning-after pill. It may show a woman in her first pregnancy, experiencing intermittent spotting of blood and sleepless nights; or a "contraction timer" used for advanced labour at 26 weeks' pregnancy.

The intimate and sensitive nature of this information makes it critical that:

- it should not be disclosed to another organisation without clear, active and unbundled consent by the consumer in respect of the specific organisation or organisations;
- it should be subject to strict security measures and deleted – not just de-identified or "isolated" – when it has served the consumer's purpose;
- if the data is released to other institutions and companies for their research purposes, consumers should be assured of strict standards of de-identification, role-based access

Table 1: Types and methods of personal data collection

Data collection type and method	Examples of such data collected by various apps analysed
Identification data sought from consumer	Name; partner's and children's names; address; email; social media login.
Symptoms logged by consumer	Menstrual cycle data (which days bleeding, spotting, no blood); cervical symptoms (cervical fluid type, position of cervix); sex drive; feelings (including angry, tired, numb, PMS, mood swings, anxious, stressed, panicking); pain (cramps, sore breasts, ovulation pain, backache, headache, painful intercourse); gastrointestinal (including vomiting, constipation, diarrhoea, gas); ailments (including urinary tract infections and sexually transmitted infections); hangover; vaginal health (including swollen, itchy); weight; contraction timing, if pregnant.
Activities logged by consumer	Sexual activity (including protected or unprotected, withdrawal, orgasm, no orgasm, vaginal, masturbation, oral sex, touching, sex toys, anal sex, none); number of servings of alcohol; smoking; birth control method; appointments with doctor or midwife; type and date of medications.
Test results logged by consumer	Ovulation test results; pregnancy test results; blood pressure.
Further questions asked through set-up, pop-ups, surveys and questionnaires	Date of birth; medical conditions (polycystic ovary syndrome, endometriosis, thyroid-related condition); relationship (including stressful, unsafe, not in a relationship); history of cancer or depression; whether exposed to sexually transmitted diseases; number of miscarriages; whether enough money to pay bills; whether utilities shut off or afraid might be hurt at home; level of insurance; education level; abnormal pap test results; due date, if pregnant.
Data about children sought from consumer	Due date, if pregnant; gender; date of birth after pregnancy; contraction timing; method of birth; older children's dates of birth.
Revealing choices by consumer in app	Articles and insights consumer focuses on (including "Why Can't I Get Pregnant?"; "What's It Like Taking Clomid for Infertility?"; "Where to Find Help as a Single Mom"); groups joined (including "Single Mom's Club"; "TTC After Recurrent Miscarriage"); questions for doctor (including "I'm gaining too much weight"; "I feel depressed"); registry style choices (including "Shopaholic" or "First-time parent essentials"); to-do list choices (including "Buy a book for first-time dads"; "Book a trip or holiday"); selection of "Pregnancy mode" or "No longer pregnant" in settings; additions to baby registry; ads clicked in app.
Data automatically collected beyond app	Extra data collected from data brokers and analysts about consumer's demographics and interests; other websites and apps used by consumer; consumer's interactions with ads on other websites and platforms.
Data automatically collected to single out and track consumer	Advertising identifier; application identifier; data from cookies and other tracking technologies, such as etags, pixels, web beacons; device identifier; device manufacturer and model; screen resolution; operating system and version; browser type and version; mobile operator and network information; device storage information; IP address; language settings; time zone; date/time stamps; location data.

controls, contractual limitations on researcher re-use of the data, and other organisational and technical forms of data security; and

- any research using the data should be carried out in accordance with recognised ethics guidelines, including Human Research Ethics Committee (HREC) approval and use of Participant Information and Consent Forms to recruit voluntary research participants.

Fertility apps' privacy practices currently reveal failures in all these aspects, as explained in later sections.

More personal questions outside logging data

Aside from logging data, fertility apps tend to ask consumers many questions about sensitive matters, in the course of setting up their account, or later on in "pop-up" questions, surveys and questionnaires. Sometimes answering these questions is mandatory before the consumer can proceed to use the app and other times the option not to answer is relatively concealed, for example, as a small, faint "Skip" or "X", in the corner of the screen. Some of this is information which may be seriously prejudicial to the consumer even if it is not health information.

The "Ovia" app, for example, presents consumers with a "Health Assessment", which explains that "[i]n partnership with health plan providers nationwide, we offer a quick health assessment to help you receive more personalized health alerts and education in the Ovia app".¹¹

Box 1 – Examples of Ovia "Health Assessment" Questions

"How many pregnancies have you had?"

"How many pregnancy losses (miscarriages) have you had?"

"Check the box if you have a history of: Endometriosis; PCOS; Uterine Fibroids; Diagnosed infertility; Multiple anormal paps; Depression; None of the above"

"Do you have a history of malignancy (cancer)?"

"Do you have painful periods?"

"Do you have a uterus?"

"In the last 12 months, did you ever eat less than you felt you should because there wasn't enough money for food?"

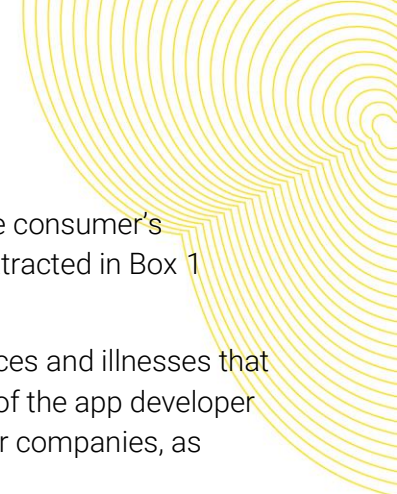
"Are you worried that in the next 2 months, you may not have stable housing?"

"How often does this describe you? I don't have enough money to pay my bills: Never; Rarely; Sometimes; Often; Always"

"In the last 12 months, have you ever had to go without health care because you didn't have a way to get there?"

"Are you afraid you might be hurt in your apartment building or house?"

"What is your highest education level?"



This lengthy questionnaire covers far more than health information, extending to the consumer's financial situation, relationship, safety and housing, as indicated by the questions extracted in Box 1 above.

These further personal questions frequently seek information about life circumstances and illnesses that are not required for the app's functions but likely serve other commercial purposes of the app developer and its commercial partners. Ovia, for example, sells "de-identified" datasets to other companies, as explained further below.¹²

Revelations from the consumer's use of the app

It would be much less obvious to consumers that the way they use the app, beyond logging data and answering questions is constantly monitored by the app developer and other organisations.¹³ **Consumers' browsing, searching, clicking and choices in the app are recorded, in part to permit the app developer and other organisations to draw inferences about further characteristics or attributes of the consumer, for their commercial purposes.** This data is often collected using cookies and various other tracking technologies set by the app developer and others when the app is launched.

Inferences could begin to be drawn from data that shows that a teenager read an article on "Surviving Sexual Assault" and joined the "Rape / Sexual Abuse Support" and "Abortion Support" groups; or that a woman joined the "Postpartum Depression" group in the app, read a series of articles on depression in the app, and clicked on an ad for a mental health app. In isolation, this data could have more than one meaning, but the strength of inferences increases with further observation of the consumer's behaviour over time and in combination with data about other websites and apps used by the consumer. Fertility apps and other organisations, such as Google Analytics, track the consumer's activities in the app and across other websites and apps.¹⁴

The "Pregnancy+" app collects data from the consumer's use of the app in various ways that would permit the app developer to draw inferences about their health symptoms, purchase intentions and family situation. These include options consumers can add to their ongoing "To Do" list in the app, as well as options the consumer can select to add to the list of "Questions: What to ask your doctor". Some of these are shown in Box 3 below.

The "What to Expect" app collects data that would permit a wide range of inferences about health, ethnicity, drug use and family situation, including potential inferences based on the "Groups" consumers choose to join on the app and the various articles the consumer reads – such as "Gestational Diabetes", "Where to Find Financial Help as a Single Mom" or "Termination for Medical Reasons" – as shown in Box 2 below.

However, the "What to Expect Privacy" policy only notes the collection of such information "about your use of the Services" under the heading of "Other Information" as opposed to "Personal Information".¹⁵ It states that, "Under certain circumstances and depending on applicable law, some of this Other Information may constitute Personal Information".

Clearly, fertility apps are collecting and using such "online activity data" or "usage data" for various purposes. But are these companies treating the resulting inferences about an individual's health or sexual orientation or sexual practices as sensitive information, and the inference itself as a collection of sensitive information? Or do they argue that these are mere "interests" on the

part of the consumer and therefore not entitled to the special treatment reserved for “sensitive information” under the *Privacy Act 1988* (Cth) (*Privacy Act*)?

Box 2 – “What to Expect” chat group options and articles

Examples of Chat Group options consumers can join:

“Plus Size Moms and Moms to Be”

“Stillbirth Support Group”

“Ectopic Pregnancy Losses”

“TTC after recurrent miscarriage”

“Gestational Diabetes”

“Termination for Medical Reasons”

“Moms of Preemies”

“Postpartum Depression”

“LGBT parents / children”

“Ganja Mamas”

“Single Moms Club”

“Partners of Porn Addicts”

Examples of articles:

“HIV or AIDS During Pregnancy”

“Where to find financial help as a single mom”

“What you need to know about child support”

“Is Yellow Discharge Normal?”

“Do Pot and Pregnancy Mix?”

“What’s it Like Taking Clomid for Infertility?”

“Why Can’t I Get Pregnant?”

“Let’s Talk about Gestational Diabetes?” (video)

“Can Dads get Postpartum Depression?”

“What’s it Like to be a Dad with Postpartum Depression?”

The uncertain status of this data under the privacy policies of fertility apps reinforces the need for clarity regarding what constitutes “personal information” and when personal information is “collected” under the *Privacy Act*.

Information that relates to an individual who is reasonably identifiable should clearly include “inferred information, including predictions of behaviour or preferences, and profiles generated from aggregated information”. Collection of information occurs when a company makes an inference about the individual, triggering the obligations regarding the treatment of personal information under the Australian Privacy Principles (APPs).

If a fertility app is using a certain category – such as “TTC after recurrent miscarriage” group membership – as a proxy for sensitive health information, that proxy itself should be treated as sensitive information.¹⁶ These matters should be clarified in the legislation itself for the avoidance of doubt, as proposed in the Privacy Act Review Report.¹⁷

Data automatically collected to single out the consumer and for tracking beyond the app

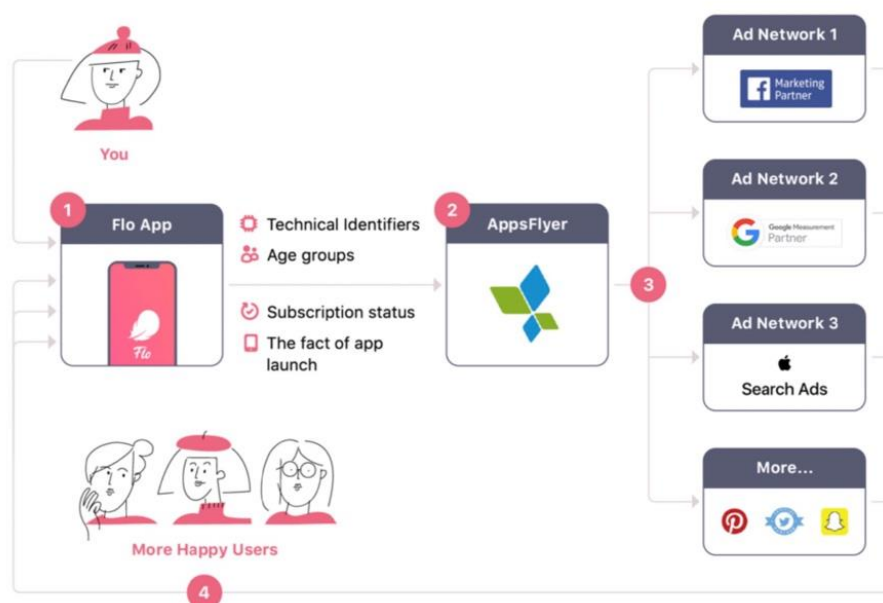
What is almost entirely hidden from the consumer are the ways in which data is collected from their device for the purpose of tracking them beyond the fertility app, as well as further data about them that the app collects from various third parties. This data collection is invisible to the consumer in their use of the app and occurs without any action or response from them, simply as a result of downloading the app and visiting certain tabs or pages.

Fertility app privacy terms also generally include some description of the automatic collection of “technical data” that allows various companies to track the consumer. However, they do this in terms that make it unlikely that consumers will understand the significance. For example, most consumers would not understand that the following description of information collected by the app could facilitate “device fingerprinting”¹⁸ to enable the app developer and other organisations to combine information about the consumer’s activities on different websites and apps, without using the consumer’s name, email, or advertising identifier:

“**Device information:** Device model; Information about the operating system and its version; Unique device identifiers (eg IDFA); Enabled device accessibility features (eg display features, hearing features, physical and motor features); Mobile operator and network information; Version of your device system. **Location Information:** IP address; Time zone; Information about your mobile service provider.”

The “Flo” app, for example, sends some such information – together with the consumer’s age group, subscription status and the fact they have launched the app – to the adtech provider, AppsFlyer.

Figure 1: Flo AppsFlyer data sharing illustration¹⁹



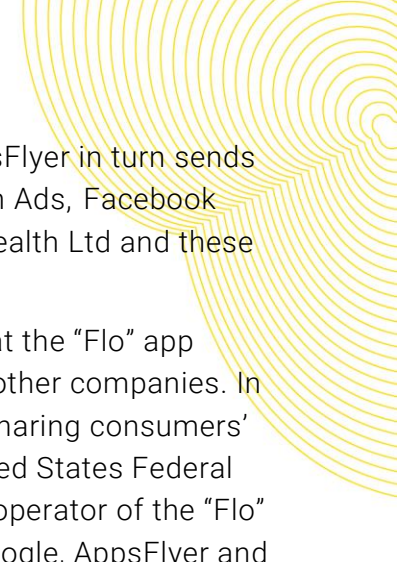


Figure 1 above is an illustration from the Flo privacy policy, showing how AppsFlyer in turn sends this information to its “partners”, including Pinterest, Google Ads, Apple Search Ads, Facebook marketing network and “others”. The privacy policy says that this allows Flo Health Ltd and these organisations “to find you or people like you on different platforms”.

This degree of transparency on Flo Health’s part follows earlier allegations that the “Flo” app misled consumers about whether and how their information was shared with other companies. In 2019, the Wall Street Journal published a story alleging that the Flo app was sharing consumers’ health information with Facebook Inc and other companies.²⁰ In 2020, the United States Federal Trade Commission (FTC) launched a complaint against Flo Health Inc, as the operator of the “Flo” app, for allegedly disclosing consumers’ sensitive health data to Facebook, Google, AppsFlyer and Flurry for years, therefore misleading consumers when it repeatedly promised the information would not be shared with anyone.²¹

Flo Health Inc subsequently reached a settlement with the FTC, which included a requirement that it obtain an independent audit of its privacy practices and transparently disclose how it shares consumer’s data with other companies, including large digital platforms.²² However, Flo app users commenced two class actions against Flo in California in 2021.²³ In 2020, a new company, Flo Health UK Ltd, was incorporated in the United Kingdom, with the Flo app founder, Dzmity Gurski, as its first director.²⁴ Flo Health UK Ltd now operates the Flo app and advertises that “[a]t no time has Flo ever sold user information, nor have we ever shared it with third parties for advertising purposes”.²⁵ It also advertises that its privacy practices have passed the scrutiny of an independent audit.

Data automatically collected beyond the app

Some app developers invisibly collect further data about the consumers from third parties, such as data brokers. For example, buried in the terms of each of the “What to Expect” and “BabyCenter” privacy policies is a list of various third parties that supply the app developer with extra information about the consumer, including data brokers, social network services and other “third parties”. The policies state that this is combined with the data collected by the app “to enhance our records” by “appending additional information to your profile”.²⁶

Such collection of extra information from third parties is likely unlawful under the existing *Privacy Act*, and particularly APP 3.6, as I have argued elsewhere.²⁷ APP 3.6 requires the company to collect information about an individual from that individual unless it is unreasonable or impracticable to do so. Where an app is already collecting information directly from an app user, it is very difficult to argue that it would be unreasonable or impracticable to ask the individual whether they are willing to provide additional data. It is more likely that the app developer seeks this information from a third party, because the individual may refuse to provide it.

The rule in APP 3.6 has never been enforced against an organisation seeking information about an individual from a data broker for its “data enrichment” purposes. APP 3.6 should be enforced. Australia’s privacy regulator should be adequately funded to effectively enforce the law.

Box 3 – Pregnancy+ “Questions” for Doctor and “To Do” List

Examples of **“Questions” for doctor options** consumers can select:

“My hands and feet are bloated. Is this a sign of pre-eclampsia?”

“I’ve lost a little blood, light spotting. Should I be concerned?”

“I have haemorrhoids. How can I relieve the discomfort?”

“I feel depressed. Is this normal? Should I be worried?”

“I can’t sleep at night. Is there anything I can do?”

“I’m gaining too much weight. Should I change my diet?”

“I have a lot more vaginal discharge. Is this normal?”

Examples of **“To Do list” options** consumers can select:

“Book an appointment with my doctor to discuss bleeding”

“Talk to friends with children about my anxiety”

“Plan a trip or holiday”

“Find out if the water is safe to drink at my holiday destination”

“Arrange a wedge-shaped pillow to elevate my head and reduce heartburn”

“Look into products to support breastfeeding”

'We never sell your data' – until we do

Five of the twelve apps analysed claim that they do not sell data or that they “never” sell data either in their privacy policies or in-app messages.²⁸ However, four of these same apps state in the fine print of the later sections of their privacy policies that the consumer’s personal information may be sold as a business asset, either on its own or as part of a sale of the whole business.²⁹ Some even say this information can be disclosed during negotiations for such a sale.³⁰ The broad description of the data that can be sold in this way would include intimate logging data and answers to prejudicial questions.³¹

For example, the “My Calendar” app by “Simple Innovation” states in its “How My Calendar Protects Your Sensitive Data” document (accessible from a link in the app) that:³²

“We do not and will never sell your data as it is against our beliefs and mission.”

However, separately, the “My Calendar” privacy policy states:³³

“If we are involved in a merger, acquisition, reorganization, restructuring, or other sale or transfer of all or any portion of our assets or business, that could involve your Personal Information and User Data being transferred to the buyer or surviving entity.” (emphasis added)

Headline statements about “not selling data” are clearly made to induce consumers to trust the service with their sensitive information. It is most unlikely that consumers would expect that Simple Innovation, in this instance, considers that it can still sell consumers’ personal information as part of a database to some other company, after such an unequivocal statement that it will “never sell your data”.

If the company intends to treat consumer’s sensitive information as a business asset, or part of a business asset, that can be sold to another entity, this should be mentioned as a clear exception alongside any “do not sell” statements. In the absence of such a clear qualification, these statements are likely to give consumers the false impression that their information will only be held by the organisation making the “do not sell” statements.

The possibility of the sale of the app business to another company in another line of business, is far from theoretical. There are numerous examples of such sales, including the purchase of the “What to Expect” and “BabyCenter” apps by the Everyday Health Group as part of the digital media corporate group, Ziff Davis;³⁴ the purchase of Ovuline Inc and its “Ovia” app by drug development and diagnostics corporate group, Labcorp; and the purchase of FitBit by Google.³⁵

Further examples of such contradictory statements about the sale of data can be found in the “Flo” app privacy policy and in-app statements. The “Flo” privacy policy states:³⁶

“No sale of Personal Data. We will not sell or rent your Personal Data. ...”

Some opening screens of the app itself state, as shown in Figure 2 below:³⁷

“Your data is yours – it will never be sold”

“Your health data will never be shared with any company but Flo ...”

The Flo Health website “Privacy Portal” page reiterates:³⁸

“When it comes to your body, we believe you deserve to be in complete control of your data. Your health data will never be shared with any company but Flo, and you can delete it at any time.”

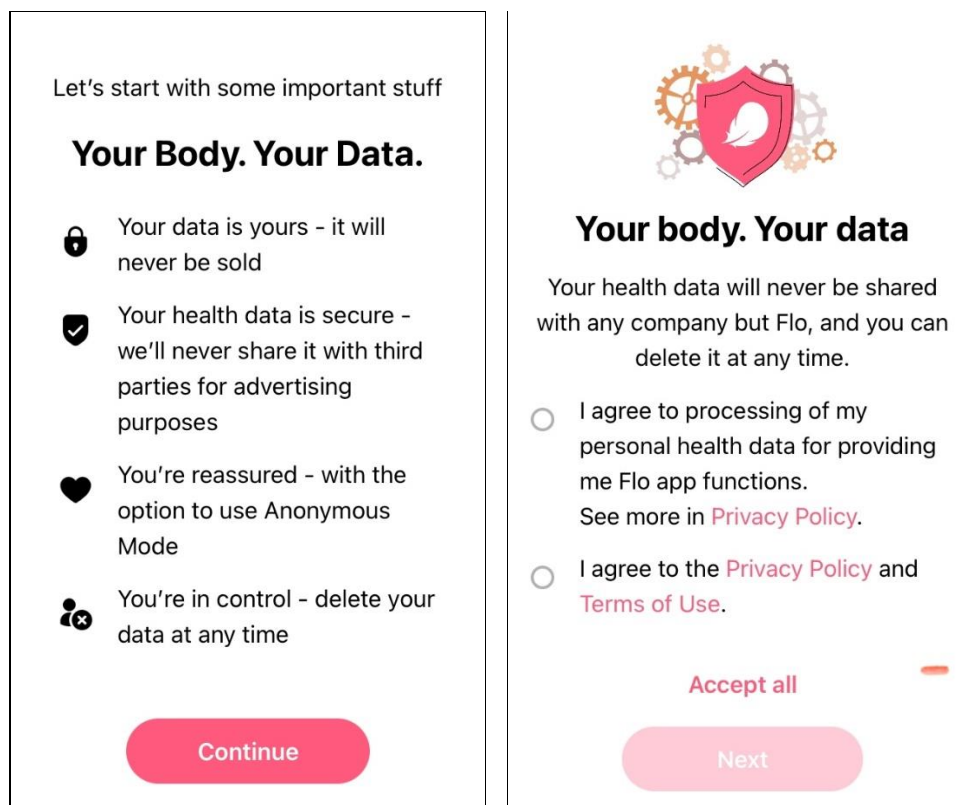
However, the Flo privacy policy separately contains a term in its later passages, which contradicts these unqualified statements:³⁹

“[I]n the event that we go through a business transition, such as a merger, divestiture, acquisition, liquidation or sale of all or a portion of its assets, your information will, in most instances, be part of the assets transferred” (emphasis added)

Flo Health UK Ltd evidently contemplates the possibility that it will sell consumers’ information as an asset in itself, or as part of a broader merger or acquisition.

Despite the clear message to the consumer that the company will not sell their personal information in any situation, each of these companies considers itself free to sell the whole database, including that consumer’s personal and sensitive information. These representations warrant scrutiny under the Australian Consumer Law, having regard to the law against misleading or deceptive conduct.

Figure 2: Flo “Data will never be sold / shared” app screens, accessed 31 January 2023



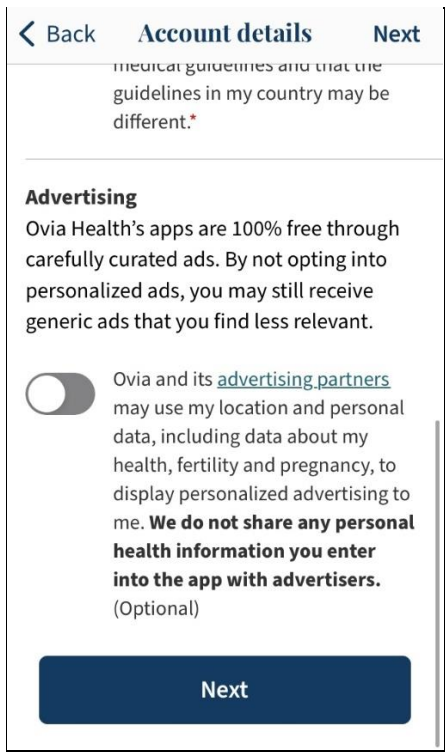
Confusing and misleading privacy choices

Some of the fertility apps analysed also provide privacy settings that are likely to give consumers misleading – or at least deeply confusing – messages about what they are choosing, on the limited occasions when consumers are permitted to make an active choice about the collection and use of their data. Two examples are provided below.

Health data is not shared, but is used by advertising partners

The “Ovia” app presents consumers with a “choice” about the use of their personal and sensitive information for advertising purposes during the account set-up process, as shown in Figure 3. Aside from the opening claim that “Ovia Health’s apps are 100% free through carefully curated ads”, the most obvious message in this choice screen is the sentence in bold, placed directly above the dark-coloured “Next” button: “We do not share any personal health information you enter into the app with advertisers.”

Figure 3: Ovia “Advertising” choice screen, accessed 7 February 2023



This is likely to create the impression that, even if the consumer agrees to “opt in to personalized ads” rather than seeing only “generic ads”, there is no danger that their personal information will be shared with the external advertising companies.

However, that may well be a false impression. The sentence immediately before the sentence in bold states: “Ovia and its advertising partners may use my location and personal data, including data about my health, fertility and pregnancy, to display personalized advertising to me.” This is a

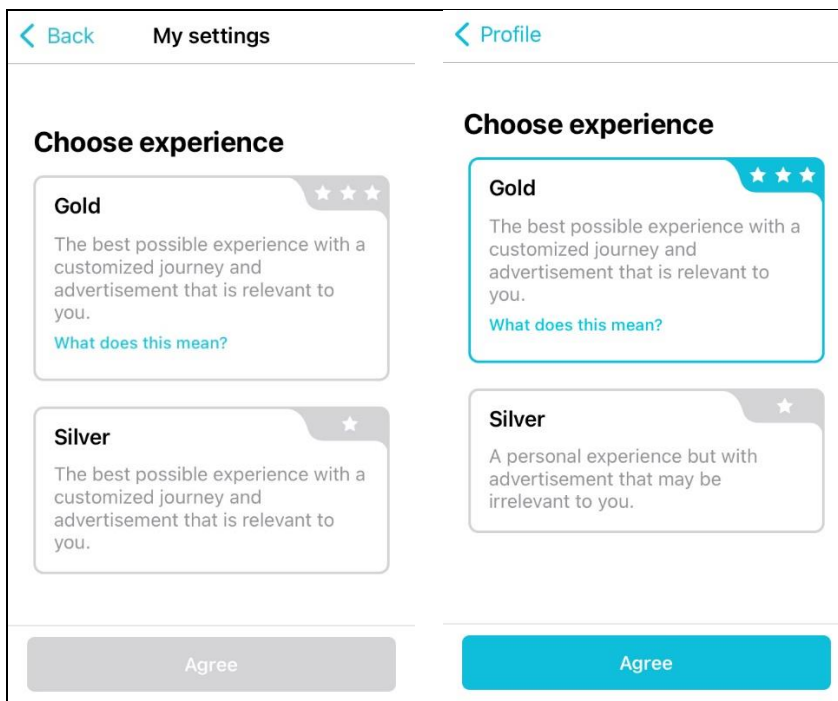
more complex sentence, which is placed further away from the action button and not in bold. The apparent contradiction is that the sentence in bold states that Ovia does “not share any health information you enter into the app with advertisers”, whereas the sentence in bold states that its “advertising partners may use ... data about my health, fertility and pregnancy, to display personalized advertising to me”.

Is one of the sentences inaccurate? Or is Ovia disclosing to advertisers only data it collects by observation or inference “about [your] health, fertility and pregnancy” but not “health information you enter in the app”? Or does Ovia claim consumers should be aware of some difference between “advertising partners” and “advertisers”? The hyperlink on “advertising partners” does not help the consumer in this respect, because it takes the consumer to a blank screen. A consumer acting upon the information in this setting cannot possibly understand the practice for which they are supposedly providing their consent.

Choose “Gold” for less privacy

In another example, the “Pregnancy+” app offers consumers a choice between two levels of membership upon registration, as shown in Figure 4. The choice screen as at 31 January 2023 displayed an identical description of both levels of membership, save that one is labelled “Gold” with three stars and one “Silver” with one star. By 21 March 2023, this setting had changed so that “Silver” membership was said to have “advertisement that may be irrelevant to you”.

Figure 4: Pregnancy+ “Gold / Silver” choice screen, accessed 31 January 2023 (left) and 21 March 2023 (right)



Either version is likely to create the impression that the “Gold” membership gives the consumer greater benefits than the “Silver” membership. If the consumer follows the “What does this mean?” link, they are merely taken to the “PREGNANCY+ and BABY+ Privacy Notice” in its entirety, with no immediate sign of any reference to “Gold” or “Silver” memberships. However, a bright blue

button is displayed at the foot of the screen, saying: "OK, count me in".⁴⁰ If this button is pressed, Gold membership is selected.

It is more than 1,100 words into the 5,500-word privacy notice that Philips reveals the difference between Gold and Silver memberships. Both memberships involve extensive tracking of how the consumer uses the app to draw inferences about their interests and preferences, as well as disclosures of consumer data to Google and the use of supposedly "anonymous information"⁴¹ collected by cookies to track the consumer's interactions with Philips ads on external websites.

The only difference is that, for Gold members, "in addition to the above, the app uses your advertising ID". This allows Philips to also show the Gold member targeted advertising "through our External Media channels, such as Facebook, Google and Pinterest" using the advertising identifier, and allows Google to "independently use your advertising ID to further personalize the advertisements shown in the app".⁴² Essentially, the consumer can be tracked and targeted more pervasively and with more certainty as to their identity if they are a Gold member.

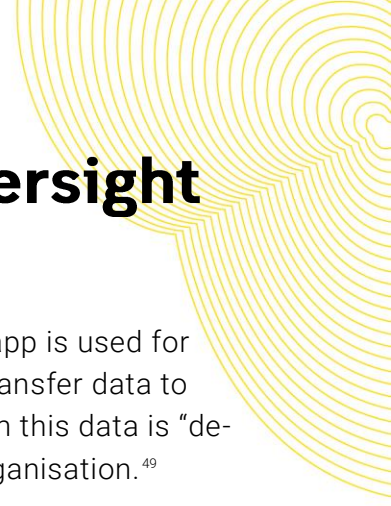
The fact that Philips conceals this difference between the two memberships in the fine print of its privacy notice, rather than providing a clear explanation in the settings, tends to suggest that Philips doubts that consumers would be attracted to this feature. This choice architecture may be seen to contain features of deceptive design or "dark patterns", that diminish the consumer's ability to make choices in their own best interests.⁴³ For example, the "What does this mean?" link resembles the "Trick Question" dark pattern in that the link fails to provide meaningful information that is relevant to the consumer's decision and the only option presented on the screen is to select the Gold membership via the "Ok, count me in" button. The presentation of the Gold and Silver options might also be seen as an example of "False Hierarchy" where Gold is presented as the unequivocally superior membership through wording and imagery. These design elements leverage the behavioural biases of framing effect, default bias and choice and information overload to lead the consumer to the preferred choice for business, which is for the consumer to consent to more data collection and sharing.⁴⁴

Implications for law reform

Neither of these choice screens should pass the test for "transparency" in the management of personal information required by APP 1.1, or the requirements for a "collection notice" under APP 5.⁴⁵ They add support to the argument that APP 5 be amended should specifically require that collection notices be "clearly expressed", as proposed in the Privacy Act Review Report.⁴⁶

These examples also weigh against proposals that consumers should have to opt *out* of further uses of their personal information if they object, for example, to use of their data for a company's targeted advertising business. Companies control the choice architecture presented to consumers, including the explanations of the respective choices, and the colour, highlighting and positioning of various elements. Consumers facing an opt-*in* choice are confronted with the challenge of these elements being designed in favour of the companies' interests and against their own. **If these methods of manipulating choice architecture are combined with the inertia created by 'default bias', there is little likelihood that opt-out rules proposed in the Privacy Act Review Report will assist consumers in guarding their own interests.**⁴⁷

This also has implications for the proposed "fair and reasonable" test, as discussed below.



"Research" uses without ethics oversight or reliable de-identification

Six of the twelve apps analysed specify that data from consumers' use of the app is used for research purposes.⁴⁸ Most of these expressly state that they also disclose or transfer data to various external researchers. The privacy policies of these apps generally claim this data is "de-identified" or "anonymised" before it is disclosed to researchers outside the organisation.⁴⁹

However, this analysis identified three trends in these research uses which jeopardise consumers' privacy and agency:

- The apps tend to be unacceptably vague about the methods of "de-identification" adopted and, in some cases, merely pseudonymise the data, such that de-identification claims may be misleading.
- Of those apps that use the consumer's data for research purposes, almost all fail to provide the consumer with an active choice in the matter.
- None of the apps promise that any research using the consumers' data will be conducted in accordance with recognised ethics guidelines or subject to approval and oversight by a Human Research Ethics Committee.

Unsafe lack of de-identification standards

Despite the extremely sensitive nature of much of the data collected, the privacy terms of the apps analysed fail to describe de-identification standards that could give consumers confidence that they are safe from being associated with that data in public or in another organisation's hands in future. The apps do not warn consumers of the risk that their data will be re-identified and associated with the individual consumer when the app developer retains or discloses the de-identified data.⁵⁰ On the contrary, some plainly state, for instance, that such data "is no longer linked or linkable to you".⁵¹

At the outset, some of the apps do not appear to de-identify the data prior to using it for research purposes, but only pseudonymize the data. That is, they replace the user's name and email address with a pseudonym such as a unique number or a hashed email address. For example, the "Clue" app privacy terms state that, for research purposes, user data is "carefully de-identified to protect your privacy", which means that:⁵²

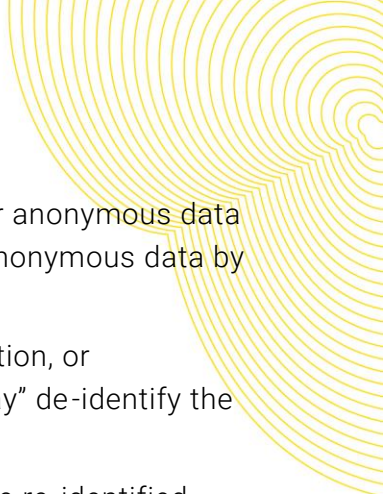
"we de-identify your personal data by removing or hashing personal identifiers so that neither the researchers nor third parties can link it to you."

This process does not result in de-identified data, but only pseudonymised data. The developer should acknowledge that this is still personal data, since the whole record could be associated with the individual if an organisation succeeds in connecting the hashed email address or other unique identifier to that person.

In other cases, the app privacy terms are **unacceptably vague about the methods used to de-identify** such comprehensive and sensitive datasets. For example, the Glow Nurture app explains in respect of its research uses:⁵³

Table 2: Claims that data is de-identified for research purposes

App	Examples of personal data collected	Description of “de-identification” for research
Clue	Name; email or social media login; due date, if pregnant; device data, including model, name and identifiers, device settings and application identifier; birth control method; sexual activity (including protected or unprotected, withdrawal, sex drive, masturbation, sex toys, orgasm or no orgasm, painful intercourse); ailments (including urinary tract infections and sexually transmitted infections).	<p>“For that purpose we de-identify your personal data by removing or hashing personal identifiers so that neither the researchers nor any third parties can link it to you.”</p> <p>“De-identification means that Clue will either delete such information from data sets that could identify you as an individual, such as your username or email address, or will replace this information with a random number, so information on your identity will not be shared with any research partner.”</p>
Glow	Name; date of birth; email; due date (or child’s birthday, once born); ultrasound photos; partner’s name; care team contact details; Apple health kit data; names of medications taken; ; vaginal health; weight; gastrointestinal symptoms; contraction timing; blood pressure; registry choices including “Shopaholic” or “First-time parent”.	<p>“As part of these activities, we may create aggregated, de-identified or other anonymous data from personal information we collect. We make personal information into anonymous data by removing information that makes the data personally identifiable to you.”</p>
Natural Cycles	Menstrual cycle data; sexual activity (including vaginal, masturbation, oral, touching, toys, anal, none); hungover; sex drive; feelings (including angry, tired, numb, PMS, mood swings, anxious, stressed); pain (cramps, sore breasts, ovulation pain, backache, headache); medical conditions (polycystic ovary syndrome, endometriosis, thyroid-related condition); sleep habits; ovulation test results; pregnancy test results.	<p>“If we have your consent, we will use your User Data and other Personal Data that you may provide, in pseudonymized or anonymized form ..., for scientific studies, scientific articles and other research purposes as may be disclosed when your Personal Data is collected. ... Natural Cycles also contributes to research carried out by selected universities, institutions and other parties by sharing anonymized and minimized data with them. For the avoidance of doubt, we do not share any Personal Data with such external parties.”</p>
Ovia	Full name; date of birth; approximate location; due date, if pregnant; menstrual cycle data; sexual intercourse; sex drive; relationship (including stressful, unsafe, not in a relationship); number of servings of alcohol; history of cancer; history of depression; whether exposed to sexually transmitted diseases; number of miscarriages; whether enough money to pay bills; whether utilities shut off or afraid might be hurt at home; level of insurance; education level; abnormal pap test results; weight; vaginal symptoms; type and date of medications taken; gender and dates of birth of other children if add Ovia Parenting & Baby Tracker App.	<p>“Deidentified data is not personal data as it is no longer linked or linkable to you. If we create a deidentified dataset we maintain it as such and will not re-identify it. We may provide deidentified data to our research partners, such as universities and medical research institutions for research, and to other businesses who have engaged us to provide research services on deidentified or aggregated data. ... Ovia may disclose or sell deidentified data derived from patient information (as defined by the California Consumer Privacy Act); if so, such patient information is deidentified in accordance with HIPAA safe harbor or expert determination deidentification requirements.”</p>



“As part of these activities, we may create aggregated, de-identified or other anonymous data from personal information we collect. We make personal information into anonymous data by removing information that makes the data personally identifiable to you.”

It is not clear whether the company is promising to de-identify all such information, or transforming it on occasion at its own discretion, since it only states that it “may” de-identify the personal information in this way “[a]s part of these activities”.

Nor can this description give the consumer confidence that their data will not be re-identified. That is, Glow’s statement that it anonymises data “by removing information that makes the data personally identifiable to you” does not clarify whether Glow only removes the consumer’s name and email address – which would be inadequate to anonymise the data – or whether it also replaces the consumer’s date of birth with an age range, and removes further information such as partner’s details, the care team’s details, and ultrasound photographs, which might be connected with the consumer.

Even where an app is specific about the method used, the de-identification method might be inadequate given the comprehensive data collected by the app, and plausible methods of re-identification. For example, Ovia states that it sells “deidentified data derived from patient information” and that this data “is deidentified in accordance with HIPAA safe harbor or expert determination deidentification requirements”.⁵⁴ Despite the reference to these standards recognised under US legislation, research has shown that the standards accepted under the Health Insurance Portability and Accountability Act (HIPAA) do not always prevent re-identification of health information.⁵⁵

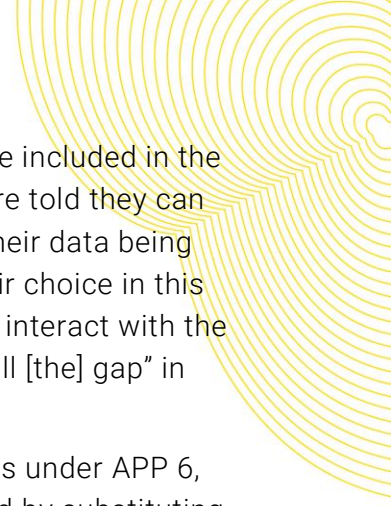
The risk of re-identification is heightened in the case of apps such as “Ovia” which may collect information about the gender and dates of birth of multiple children of one mother, together with the mother’s date of birth. As Culnane, Rubinstein and Teague have explained, even where the mother’s date of birth is reduced to a year of birth or age range, dates of birth for more than one child of the same mother are likely to permit identification of a unique individual.⁵⁶

Even where only one child’s date of birth is recorded in combination with the birth mother’s age range and approximate location, there may be a significant risk of re-identification if the mother is below a certain age or above a certain age, such that relatively few people have given birth at that age.⁵⁷ These possibilities are just a couple of examples of the ways in which a very small number of data points can be used to re-identify a record. The same may be true for a few points of precise location data or a combination of prescribed pharmaceuticals.

Lack of consumer choice about use of their data in research

The real risks of re-identification outlined above, together with the extreme sensitivity of some of the data collected, make it vital that consumers should be permitted to make an informed choice about whether they are willing to accept these risks for the sake of the additional research purposes explained to them. However, six of the apps which use consumer’s data for some form of “research” do so by default without allowing the consumer to decide whether to opt into that research use.⁵⁸ Of those, five do not provide the consumer with an opt-out for the research use.⁵⁹

By contrast, the “Natural Cycles” app does not opt consumers into its research purposes by default but leaves this as an “unticked” option in the privacy settings of the app.



While the “Clue” app allows consumers to contact Clue if they do not want to be included in the research, there is no opt out setting provided in the app. Instead, consumers are told they can contact Clue at the email address provided if they are “not comfortable” with their data being used for this purpose.⁶⁰ This creates obstacles for consumers in exercising their choice in this respect, both because of the time and effort required and the potential need to interact with the organisation over this choice, when it has indicated that it is “on a mission to fill [the] gap” in female health research “by sharing user data”.⁶¹

It is difficult to see how such an approach complies with the entity’s obligations under APP 6, particularly if the data remains in its raw state or has only been pseudonymised by substituting an identifier for the consumer’s name and email address. APP 6.1 requires the individual’s consent to any use of sensitive information for a secondary purpose that is not directly related to the primary purpose (as is the case with such research uses) and this should be express consent.⁶²

Lack of ethics oversight or adherence to ethics guidelines

Aside from the failure to provide clear information and real choices for consumers about use of their sensitive records for research purposes, consumer interests are not protected by adherence to some recognised ethics guidelines and submission to approval by a HREC.

None of the apps that use data for research purposes promise that any research using the consumer’s data will be conducted in accordance with recognised ethics guidelines or subject to such ethics oversight. Nor do the app developers promise that all external organisations receiving that data for research purposes will comply with recognised ethics guidelines or be subject to ethics oversight.

Accordingly, there are no clear rules about how the parties will collect, store, protect and delete the data, having regard to the remaining risk of re-identification. There is also no assurance regarding the ethics of the purposes of that research and its potential consequences for certain groups who might be affected by it. Clue, for example, only promises that “we personally select our scientific collaborators with the utmost care”.⁶³ However, its descriptions of its research uses for the data include “academic, clinical or internal research” in addition to “scientific and medical research about reproductive health”. Its actual research uses have extended to a “partnership” with the cosmetics brand, L’Oreal, “to deepen knowledge on the relationship between skin health and the menstrual cycle”.⁶⁴

The “Ovia” app goes further and specifies in its privacy policy that it has the right to sell de-identified data derived from patient information, without any limitation as to who may purchase that data.⁶⁵

While many consumers may associate research uses with the improvement of women’s health and benefits to women more broadly, there is currently little to stop the various researchers from using the relevant data in ways that do not create any benefits for women and could even lead to disadvantage. What if the data reveals certain consumers’ willingness to pay more for in-app purchases or other goods or services when they are at a certain stage in their menstrual cycle or their pregnancy? Or that people who experience certain combinations of PMS and physical symptoms are more likely to experience strong cravings for a particular type of fast food? Consumers should be protected from such unregulated “research” uses of their sensitive data.

Pervasive tracking and profiling

Use of consumer data for advertising businesses

All but one of the apps analysed state that they use some of the consumer's data for targeted advertising purposes. The very brief privacy policy for the "WomanLog" app is the exception in not mentioning any use for advertising purposes.⁶⁶

"Euki" is an example of a period-tracking and fertility information app that shares no personal information with any other organisation, which was not included in this analysis. "Euki" was launched in the US following the reversal of *Roe v Wade*, and there is no data available regarding its use in Australia.

Types of data used for advertising businesses

Most of the fertility apps emphasise that they do not share the consumer's health data or "data that you track in the app" with advertising companies. However, they do not highlight the data that is used for the purposes of their own and/or other advertising businesses. These include data about the consumer's use of the app, data automatically collected to single out the consumer and data collected from third parties, such as data brokers.

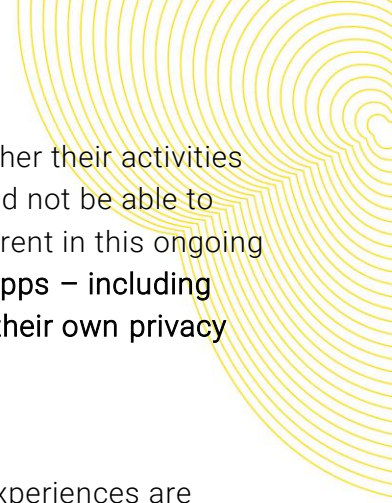
The "360-degree view" of the consumer

The data collected by popular fertility apps should not be viewed in isolation, but as part of the broader context in which consumers are subjected to pervasive surveillance for commercial purposes. This is, in truth, a striking illustration of "surveillance capitalism" in which individual's intimate life experiences are tracked, combined and scrutinised to make inferences and predictions, in the service of targeted or behavioural advertising businesses.⁶⁷

To be clear, the problem is not only that consumers are targeted with content and advertising, which may cause detriment to them and the community they live in.⁶⁸ It is also problematic that individuals' lives are continually monitored and analysed for the purposes of these businesses, whether they see targeted advertising themselves or whether their experiences are pervasively collected, analysed and disclosed to create "lookalike audiences" and improve the predictive power of these businesses' targeting algorithms.

Some large digital platforms claim that they put the consumer "in control" by allowing the consumer to opt out of *seeing* or *receiving* targeted content or advertising.⁶⁹ But they do not offer consumers a choice about whether their activities will nonetheless be monitored and analysed – and combined with data about them collected from other companies – in the service of that advertising business. Far more concerning, the Attorney General's Department recently expressed the view in the Privacy Act Review Report that this should be regarded as an acceptable and lawful restriction on individuals' privacy choices, explaining its proposal in respect of the use of personal information for targeted advertising purposes:⁷⁰

"Individuals would be able to make a choice not to see targeted advertising, but platforms would be able to collect and use information relating to [those] individuals for targeting purposes such as generating audience insights and targeting of similar users who have not elected to opt-out of receiving targeted advertising."



The Report does not explain why consumers should have no choice as to whether their activities are pervasively monitored to support advertising businesses or why they should not be able to guard against the increased risk of data breaches affecting them which is inherent in this ongoing collection and use of their information. **There are numerous examples health apps – including some fertility apps – disclosing sensitive data to other organisations, against their own privacy messaging.**⁷¹

Examples of commercial uses

This section provides some examples of the ways in which consumers' lived experiences are appropriated by companies and combined with data collected by various other organisations to create the coveted "360-degree view" of the consumer.

"What to Expect" – selling, renting and licensing data

In case the following summary creates an impression of transparency that does not exist, it should be noted that this 330-word description is based on a careful and time-consuming analysis of the 10,693-word "What to Expect" privacy policy and the various choice screens and privacy messages within the app itself. It is highly unlikely that this picture of the app developer's data practices would be apparent to the average consumer.

The "What to Expect" app collects extensive information about the consumer including: their email; precise location data; date of birth; due date; children's genders and dates of birth; how the children arrived (vaginal birth, caesarean birth, partner gave birth, adopted or surrogate); whether the consumer is a first-time parent or having twins; which articles they read on sex and fertility topics; which groups they join based on health issues and family situations (see Box 2 above); and their contributions to group chats. The article and group pages the consumer visits on the "What to Expect" app are connected with "pages you visit on other Channels", which include third party websites, apps, platforms and other media channels.

However, the fine print of the "What to Expect" privacy policy also states that it will collect further personal information from third parties, including data brokers, data aggregators, referral sources, network operators and social network services, and that it does this "to enhance our records", such as by "appending additional information to your profile". This may include information about both online and offline activities of the consumer. All this information is combined and analysed, in part to create groups and segments based on "interests" inferred from consumers' data relating to demographics, interests, pages viewed, links clicked and search terms used.

Everyday Health Inc (and its parent company Ziff Davis) use this information for numerous commercial purposes including:⁷²

- licensing segments of "User Information" to other companies;
- selling data collected through cookies and various other tracking technologies to other companies such as advertisers for their targeted advertising;
- allowing those other companies to combine that data with their own data about the consumer "to form a more detailed picture";
- providing other companies with a "lead generation" service using the consumer's data, to improve those companies' "target marketing campaigns"; and

- Everyday Health's own targeted advertising purposes.

Everyday Health appears to treat information about consumers' daily lives through their pregnancy as "stock in trade".

Your "trimester and relation" are sent to Google

Several of the fertility apps analysed indicate that they share some of the consumer's data with large digital platforms, including Google Analytics or Google Ads. The fine print of the Pregnancy+ privacy policy explains that:⁷³

"Information about how the apps are set up, such as trimester and relation, along with analytics events and unique identifiers ... is sent to Google in order to make advertisement and content more personalized and as relevant as possible." (emphasis added)

And separately:

"Google may combine information collected via the apps, with other information it has independently collected from other services and products. ... You may receive advertising about products and services not related to Philips or the mother & childcare domain."

'Relation' refers to the app user's relationship to the expected child.

Similarly, the app developer Abishkking Ltd explains in respect of its "Period Calendar" app, that Google Analytics collects data to track consumers' use of its app and that:⁷⁴

"This data is shared with other Google services. Google may use the collected information to contextualize and personalize the ads of its own advertising network." (emphasis added)

The data collected by Google Analytics via the Period Calendar app includes location, device information and "app usage data".

How might it be within the reasonable expectations of a consumer that information about their pregnancy or use of a period tracker would be used not just for the purposes of the app's targeted advertising but as an input for the world's largest and most lucrative advertising business, for use across its vast advertising network?

These examples add to evidence in support of a "fair and reasonable" test for data practices, which can take into account the broader context of an entity's data practices, including the transparency of the practices; the sensitivity of the information; and the reasonable expectations of the consumer, rather than depending on spurious claims of notice and implied consent about unacceptable data practices which remain invisible to the consumer.⁷⁵

Unsafe retention of consumers' data

A critical factor in securing sensitive data is how long that information is retained and what happens to it once the retention period expires.⁷⁶ Personal information should only be kept for as long as it is necessary to meet the lawful purposes for which it was collected. Organisations holding personal information should have a clear system for determining how long different types of data should be kept and deleting the data when it is no longer needed for those lawful purposes, in the absence of earlier deletion at the request of the consumer.

A number of the fertility apps analysed do not meet these standards, but expose the data collected to greater risk by keeping it for arbitrary and unnecessarily long periods or failing to specify any clear system regarding the retention of data.

As indicated by Table 3, the fertility app privacy policies specify retention periods ranging from three years to seven years. An exception is the “What to Expect” privacy policy, which at one point specifies a retention period of 180 days (approximately six months) but makes an exception which means the personal data is always likely to be kept for longer than six months.⁷⁷

While some of the apps permit consumers to request deletion of their data, this is not a substitute for the company itself having systems in place to delete the unnecessary data of its own accord. As a matter of practicality, it would be unreasonable to expect individual consumers to manage the deletion of all their personal data from various organisations. These apps, in particular, may span different stages of life and family situations.

Consider the “Ovia Ovulation and Period” app. A teenager might begin entering data when she is 16 years old and record years of information about her period, when she has sex and whether she used protection, her relationships, whether she has been exposed to sexually transmitted diseases, servings of alcohol consumed, moods, medications, and pregnancy test results. By default, all this information would still be held by Ovuline Inc seven years after she ceases to use the “Ovia” app, making it vulnerable to data breaches for that extensive period.⁷⁸

Many of the privacy terms of the apps analysed also fail to specify what will be done to the data at the end of that period. Given the risks associated with re-identification explained earlier in this report, this is a case where the organisation should promise to delete the data at the end of the retention period. However, several of the app privacy terms instead state that the data will then only be “de-identified” or “isolated from further processing”.⁷⁹

These failings highlight the need for tighter regulation concerning the security measures used to protect personal information, including the need for limited retention periods and the deletion of information on the expiry of those periods or sooner if the consumer makes a request for erasure.⁸⁰ These security measures should be appropriate to the risk inherent in the data practices. In the case of fertility apps, this includes real risks of harm, where highly detailed and sensitive records of an individual’s health, sexual activities and daily habits are kept and combined over time.

Table 3: Specified default periods for retaining consumer data after inactivity

App	Specified default retention period, if any, after inactivity in the absence of consumer-initiated deletion or legal requirement to retain	Deletion promised at end of retention period?
Clue	"We do not retain your data in an identifiable format for longer than necessary to deliver our services."	UNCLEAR, but data is deleted if consumer contacts Clue to request deletion.
Flo	3 years after inactivity or deletion of the app	NO. Flo will "anonymize or otherwise de-identify your data where possible".
Glow	"To determine the appropriate retention period for personal information, we may consider factors such as the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure, the purposes for which we process your personal information, and whether we can achieve those purposes through other means, and the applicable legal requirements."	NO. Glow may either "delete it, anonymize it, or isolate it from further processing".
My Calendar	"only for so long as We have a legitimate business purpose in keeping such data, as may be allowed by applicable laws."	UNCLEAR, but data is deleted if consumer uses "Delete all data" or "Delete account" feature.
Period Calendar	None specified.	UNCLEAR, but data is deleted if the consumer sends "a request through the feedback form".
Natural Cycles	3 years after consumer terminates the account (not after inactivity).	NO. Data is "anonymized".
Ovia	7 years after inactivity.	YES. Ovia promises to "automatically delete" the data after this period.
Pregnancy+	3 years and 3 months after inactivity.	YES. Data is deleted.
Pregnancy Tracker	None specified.	NO. Not specified.
WomanLog	None specified	NO. Not specified.
What to Expect	"as long as is necessary in connection with the purposes set out in this Policy"	NO. Implies data may be de-identified.



Concluding remarks

Fertility apps collect the kind of intimate data consumers that we would only usually share with our partners, doctors or our very closest friends and family: immensely information about menstrual cycles, pregnancies, health conditions, emotions and sexual activities. They may be used by consumers at vulnerable moments in their lives, when they are trying to conceive, manage unexpected health conditions, or monitor concerning developments in their pregnancy. Some of these apps are intended for use by children as young as 13.

This research provides evidence of serious privacy flaws in popular fertility apps. Unfair and unsafe privacy practices of the apps include:

- confusing and misleading privacy messages;
- pervasive tracking of the consumer's online behaviour, without clarity about whether inferences drawn from this will be treated as sensitive information;
- lack of choice about further uses of their data, including pervasive tracking for advertising businesses and research uses;
- inadequate de-identification of sensitive data shared with other organisations;
- use of the consumer's sensitive data for poorly defined "research" purposes, which do not depend on HREC approval; and
- retention health data for years after the consumer stops using the app, creating entirely unnecessary risks of data breaches.

These unfair and unsafe practices underscore the urgent need for updated privacy laws to address the data privacy risks consumers too often face, including amendments to clarify and improve the scope of information covered by the *Privacy Act* taking into account the realities of modern data practices; what choices consumers can make about their data and how; what data uses are prohibited; what security systems, including technical and organisations measures, organisations should have in place; and a test based on fairness and reasonableness, rather than spurious and mechanistic concepts of notice and consent which organisations have used to disadvantage consumers for too long.

The unfair and unsafe privacy practices of fertility apps illustrate the extent to which modern data practices disregard the value and importance of privacy, which is fundamentally concerned with the dignity and autonomy of humans. Consumers should be able to make use of technology that aids in understanding their fertility; to help them manage these precarious, joyful – sometimes heart-breaking – aspects of their lives, without sacrificing their dignity and autonomy.



Appendix

Methodology

This research seeks to determine the extent to which fertility apps commonly used by Australian consumers protect consumers' privacy, having regard to the quality of information and choices they give consumers about their data practices, as well as the extent to which they indicate that they restrict the collection, use, disclosure and storage of personal data to limit the risk that the consumer will be humiliated, excluded, exploited or exposed to potential data breaches.

The study uses the privacy terms, messages and settings of these apps to determine the quality of information and choices about data practices, and as a proxy for the extent to which the app developer's actual data practices restrict the collection, use and disclosure of personal data. No interviews, audits or traffic flow analyses were conducted. The terms presented are taken to reflect the actual data practices for the purposes of this research.

These aspects were analysed between January and March 2023 for 12 of the most popular fertility apps used by Australian consumers. I use the term 'fertility apps' to cover mobile apps that assist consumers in tracking their menstrual cycles, ovulation and potential "fertile windows" if they are attempting to conceive, and stages of pregnancy up to birth. The consumer is intended to transition through different "modes" of the one app – for example, from "Period tracking" to "Trying to conceive" to "Pregnancy" mode and back – or through different apps serving these purposes under the one brand, with the consumer directed to download the next app or use the next mode according to their changing needs in managing their fertility.

To ensure the relevance of the research for consumers, the research focused on 12 of the most popular fertility apps, as indicated by a combination of downloads and active usage of the app in Australia in the six months up to March 2023, using data from data.ai. The apps analysed, the app developer or seller, the fertility modes included, and the relevant version of the privacy policy are listed in Table 4 below. The user interface for each app was observed in both the iOS and Android versions of the app.

The study does not include apps which require connection to a wearable device like an Apple watch or a FitBit that track biometric data directly, using sensor technology; or apps which track a baby's development from birth. These raise different and important issues, which deserve to be considered separately. Stand-alone "contraction timer" apps were also excluded as serving a much more limited function for a more limited period.

This research included a systematic analysis of:

- the currently available privacy policies of each app;
- any additional privacy messaging on the app developer's website; and
- the user interface of the app itself, including the steps required to use the app, questions asked of the consumer through the app, and privacy settings (if any) available in the app.

The set of questions which form the basis of this analysis were informed by issues under consideration in the Privacy Act Review and known consumer concerns regarding personal data practices revealed by several surveys from recent years.

Table 4 – Fertility apps analysed

App	App developer / Seller (Headquarters)	Modes	Privacy Policy Version (Last update)
BabyCenter 	Everyday Health Inc (United States)	Pregnancy	October 2022
Clue 	Bio Wink GmbH (Germany)	Period Conceive	25 May 2022
Flo Health 	Flo Health UK Ltd (United Kingdom)	Period Conceive Pregnancy	14 September 2022
Glow / Eve 	Upwards Lab Holdings Inc (United States)	Period Conceive Pregnancy	1 January 2023
My Calendar 	App Manage Group #1 Simple Innovation	Period Conceive Pregnancy	19 August 2022
Natural Cycles 	NaturalCycles Nordic AB (Sweden)	Period Conceive Pregnancy	30 June 2022
Ovia 	Ovuline Inc (United States)	Period Conceive Pregnancy	21 December 2022
Period Calendar 	Abishkking Ltd (Hong Kong)	Period Conceive Pregnancy	13 September 2022
Period Tracker 	GP Apps (United States)	Period Conceive	Undated
Pregnancy+ 	Philips Consumer Lifestyle BV (Netherlands)	Pregnancy	9 May 2022
WomanLog 	Pro Active App SIA (Latvia)	Period Pregnancy Menopause	22 April 2022
What to Expect 	Everyday Health Inc (United States)	Pregnancy	10 October 2022



¹ See, eg, Privacy International, 'No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data' (9 September 2019); Catherine Roberts, 'These Period Tracker Apps Say They Put Privacy First. Here's What We Found.' (25 May 2022) *Consumer Reports*; Najd Alfawzan et al, 'Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis' (2022) 10(5) *JMIR mHealth and uHealth* 1; Mozilla, 'Reproductive Health', *Privacy Not Included* (Web Page) <https://foundation.mozilla.org/en/privacynotincluded/categories/reproductive-health/>; Megha Rajagopalan, 'Period Tracker Apps Used By Millions Of Women Are Sharing Incredibly Sensitive Data With Facebook' (10 September 2019) *BuzzFeed.News*.

² See Attorney General, 'Attorney General Becerra Announces Landmark Settlement Against Glow, Inc. – Fertility App Risked Exposing Millions of Women's Personal and Medical Information' (Press Release, 17 September 2020); 'In the Matter of Flo Health, Inc.', Flo Health Inc. (United States of America Before the Federal Trade Commission, 1923133); Federal Trade Commission, 'Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data' (Press Release, 13 January 2021); Federal Trade Commission, 'FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others' (Press Release, 22 June 2021); Kendall Heebink, 'Flo Health Files Response to Amended Class Action Complaint' (10 August 2022) *Law Street*.

³ See Attorney-General's Department, 'Privacy Act Review: Report 2022' 1.

⁴ See, eg, Frost & Sullivan, 'Femtech – Time for a Digital Revolution in the Women's Health Market' (31 January 2018) www.frost.com/frost-perspectives/femtechtime-digital-revolution-womens-health-market/; Farah Nayeri, 'Is "Femtech" the Next Big Thing in Health Care?' (The New York Times online, 7 April 2021) www.nytimes.com/2021/04/07/health/femtech-women-health-care.html

⁵ Although a number of fertility apps specifically warn that they cannot be relied upon as a method of contraception.

⁶ See, eg, Queensland Fertility Group, 'Warning about the accuracy of fertility apps used by thousands of women to help in 'baby making' (Media Release, 17 September 2019); Anna Broad, Rina Biswakarma and Joyce C Harper, 'A survey of women's experiences of using period tracker applications: Attitudes, ovulation prediction and how the accuracy of the app in predicting period start dates affects their feelings and behaviours' (2022) 18 *Women's Health* 1

⁷ Consumer Policy Research Centre, 'CPRC 2020 Data and Technology Consumer Survey' (2020).

⁸ OAIC, 'Australian Community Attitudes to Privacy Survey 2020' (September 2020) 28-37.

⁹ Roy Morgan, 'Consumer Views and Behaviours on Digital Platforms: Final Report prepared for Australian Competition & Consumer Commission' (November 2018) 17-23.

¹⁰ Roy Morgan, 'Consumer Views and Behaviours on Digital Platforms: Final Report prepared for Australian Competition & Consumer Commission' (November 2018) 17-23.

¹¹ "Ovia Fertility" in-app message in iOS version, accessed 7 February 2023.

¹² Ovia Health Apps Privacy Policy (updated 21 December 2022).

¹³ See Joseph Turow et al, 'Americans Can't Consent to Companies' Use of their Data' (Report, February 2023).

¹⁴ See, eg, 'BabyCenter Privacy Policy' (updated October 2022); 'Glow Privacy Policy' (updated 1 January 2023); 'What to Expect Privacy Policy' (updated 10 October 2022); 'Pregnancy+ and Baby+ Privacy Notice' (updated 9 May 2022).

¹⁵ What to Expect Privacy Policy (updated 10 October 2022).

¹⁶ See Office of the Victorian Information Commissioner, 'Submission by the Office of the Victorian Information Commissioner in Response to the Attorney General's Department Privacy Act Review Discussion Paper' (21 December 2021) 2.

¹⁷ Attorney-General's Department, 'Privacy Act Review: Report 2022', 29-30.

¹⁸ Shanika W., 'A Complete Guide to Browser Fingerprinting – What It Is and How It Affects You' *Privacy Affairs* (Web Page) <https://www.privacyaffairs.com/browser-fingerprinting/>

¹⁹ Flo Privacy Policy (updated 14 September 2022).

²⁰ Sam Schechner and Mark Secada, 'You Give Apps Sensitive Personal Information. Then They Tell Facebook' (*Wall Street Journal* online, 22 February 2019) https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636?mod=article_inline

²¹ 'In the Matter of Flo Health, Inc.', Flo Health Inc. (United States of America Before the Federal Trade Commission, 1923133) https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf

-
- ²² Federal Trade Commission, 'Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data' (Press Release, 13 January 2021); Federal Trade Commission, 'FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others' (Press Release, 22 June 2021).
- ²³ Kendall Heebink, 'Flo Health Files Response to Amended Class Action Complaint' (10 August 2022) *Law Street* <https://lawstreetmedia.com/news/health/flo-health-files-response-to-amended-class-action-complaint/>
- ²⁴ Opencorporates: Flo Health UK Ltd entry (Web Page) <https://opencorporates.com/companies/gb/12898410>
- ²⁵ Flo, 'Your body. Your Data' (Web Page) <https://flo.health/privacy-portal>
- ²⁶ The "BabyCenter" and "What to Expect" apps are both owned by Everyday Health Inc (a subsidiary of Ziff Davis Inc) and have almost identical privacy policies.
- ²⁷ Katharine Kemp, 'Australia's Forgotten Privacy Principle: Why Common 'Enrichment' of Customer Data for Profiling and Targeting is Unlawful' (20 September 2022) <https://ssrn.com/abstract=4224653>
- ²⁸ Clue in-app message, 1 February 2023 ("We never have and never will sell your data"); Flo in-app message, 31 January 2023 ("Your data is yours – it will never be sold"); Natural Cycles Privacy Policy (updated 30 June 2022) ("Natural Cycles never sell your Personal Data ..."); SimpleInnovation, 'How My Calendar Protects Your Sensitive Data' (Web Page) <https://www.simpleinnovation.us/my-calendar/how-we-use-data> ('We do not and will never sell your data as it is against our beliefs and mission.');
- ²⁹ Period Calendar in-app message, 10 February 2023 ("We NEVER sell your personal information.");// Flo Privacy Policy (updated 14 September 2022); My Calendar – Simple Innovation Privacy Policy (updated 19 August 2022); Natural Cycles Privacy Policy (updated 30 June 2022); Period Calendar – Abishkking Ltd Privacy Policy (updated 13 September 2022).
- ³⁰ See, eg, Period Calendar – Abishkking Ltd Privacy Policy (updated 13 September 2022).
- ³¹ Only one of the apps analysed states that the company will give the consumer a choice about whether their data will be sold to the new entity in this way or notice of the intended sale followed by an opportunity to export and delete their data prior to the sale: Period Calendar – Abishkking Ltd Privacy Policy (updated 13 September 2022).
- ³² SimpleInnovation, 'How My Calendar Protects Your Sensitive Data' (Web Page) <https://www.simpleinnovation.us/my-calendar/how-we-use-data>
- ³³ My Calendar – Simple Innovation Privacy Policy (updated 19 August 2022).
- ³⁴ 'Everyday Health Group Acquires BabyCenter' (Web Page) <https://www.everydayhealthgroup.com/in-the-news/babycenter#about>
- ³⁵ Conor Hale, 'Labcorp moves deeper into "femtech" with deal for digital pregnancy platform provider Ovia Health' (Fierce Biotech online, 13 August 2021) <https://www.fiercebiotech.com/medtech/labcorp-snags-digital-pregnancy-platform-provider-ovia-health>
- ³⁶ Flo Privacy Policy (updated 14 September 2022).
- ³⁷ Flo in-app message, 31 January 2023.
- ³⁸ Flo, 'Your body. Your Data' (Web Page) <https://flo.health/privacy-portal>
- ³⁹ Flo Privacy Policy (updated 14 September 2022).
- ⁴⁰ The blue button was observed in the iOS version of the "Pregnancy+" app, but not in the Android version of the app.
- ⁴¹ It seems very unlikely that these cookies are collecting "anonymous information" if Philips is using it to determine "how you interact with the Ad and our partner's website". It is much more likely that the information is linked back to the consumer who interacted with the advertisement within the app.
- ⁴² Pregnancy+ and Baby+ Privacy Notice (updated 9 May 2022).
- ⁴³ See Daniel Khanemann, *Thinking Fast and Slow* (Penguin Press, 2012); Chandni Gupta, 'The Choice Mirage: How Australian Consumers are Being Duped Online via Dark Patterns' (2022) 30 *Australian Journal of Competition & Consumer Law* 241.
- ⁴⁴ See Chandni Gupta, 'The Choice Mirage: How Australian Consumers are Being Duped Online via Dark Patterns' (2022) 30 *Australian Journal of Competition & Consumer Law* 241, 241-243.
- ⁴⁵ See Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise, 'Submission on the Privacy Act Review Discussion Paper' (10 January 2022) 18.
- ⁴⁶ Attorney-General's Department, 'Privacy Act Review: Report 2022', 96-97.
- ⁴⁷ Attorney-General's Department, 'Privacy Act Review: Report 2022', 213.
- ⁴⁸ BabyCenter Privacy Policy (updated October 2022); Clue Privacy Policy (updated 25 May 2022); Flo Privacy Policy (updated 14 September 2022); Glow Privacy Policy (updated 1 January 2023); Ovia Health Apps Privacy Policy (updated 21 December 2022);

What to Expect Privacy Policy (updated 10 October 2022). Natural Cycles Privacy Policy (updated 30 June 2022) may also use data for research purposes but only if the user actively opts in.

⁴⁹ See Table 2 below.

⁵⁰ See Chris Culnane, Benjamin I P Rubinstein and Vanessa Teague, 'Health Data in an Open World: A Report on Re-identifying patients in the MBS / PBS Dataset and the Implications for Future Releases of Australian Government Data' (University of Melbourne, 18 December 2017); Luc Rocher, Julien M Henrickx, Yves-Alexandre de Montjoye, 'Estimating the success of re-identifications in incomplete datasets using generative models' (2019) 10(1) *Nature Communications*; Latanya Sweeney et al., 'Re-identification Risks in HIPAA Safe Harbor Data: A study of data from one environmental health study' (2017) *Technology Science*.

⁵¹ Ovia Health Apps Privacy Policy (updated 21 December 2022).

⁵² Clue Privacy Policy (updated 25 May 2022).

⁵³ Glow Privacy Policy (updated 1 January 2023).

⁵⁴ Ovia Health Apps Privacy Policy (updated 21 December 2022).

⁵⁵ See Latanya Sweeney et al., 'Re-identification Risks in HIPAA Safe Harbor Data: A study of data from one environmental health study' (2017) *Technology Science*.

⁵⁶ Chris Culnane, Benjamin I P Rubinstein and Vanessa Teague, 'Health Data in an Open World: A Report on Re-identifying patients in the MBS / PBS Dataset and the Implications for Future Releases of Australian Government Data' (University of Melbourne, 18 December 2017).

⁵⁷ Chris Culnane, Benjamin I P Rubinstein and Vanessa Teague, 'Health Data in an Open World: A Report on Re-identifying patients in the MBS / PBS Dataset and the Implications for Future Releases of Australian Government Data' (University of Melbourne, 18 December 2017).

⁵⁸ BabyCenter Privacy Policy (updated October 2022); Clue Privacy Policy (updated 25 May 2022); Flo Privacy Policy (updated 14 September 2022); Glow Privacy Policy (updated 1 January 2023); Ovia Health Apps Privacy Policy (updated 21 December 2022); What to Expect Privacy Policy (updated 10 October 2022).

⁵⁹ Only Clue Privacy Policy (updated 25 May 2022) states that users can contact the app developer if they are "uncomfortable" with use of their data for research purposes. Natural Cycles Privacy Policy (updated 30 June 2022) may use data for research purposes but only if the user actively opts in as a distinct choice.

⁶⁰ Clue Privacy Policy (updated 25 May 2022).

⁶¹ Clue Privacy Policy (updated 25 May 2022).

⁶² The research purposes of these app developers do not fall within the exceptions for 'permitted health situations' in *Privacy Act 1988* (Cth) section 16B or the exceptions in respect of public health or safety under section 95A.

⁶³ Clue Privacy Policy (updated 25 May 2022).

⁶⁴ L'Oréal, 'L'Oréal partners with Clue, the period tracking app, and a leader in femtech, to advance scientific knowledge on the relationship between skin health and the menstrual cycle.' (Press Release, 4 August 2021) <https://www.loreal.com/en/press-release/group/loreal-partners-with-clue/>

⁶⁵ Ovia Health Apps Privacy Policy (updated 21 December 2022).

⁶⁶ WomanLog Privacy Policy (updated 22 April 2022).

⁶⁷ See Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile, 2019).

⁶⁸ See Ryan Calo, 'Digital Market Manipulation' (2014) 82 *George Washington Law Review* 995; Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy and Manipulation' (2019) 8 *Internet Policy Review*; Danielle Keats Citron, 'Intimate Privacy in a Post-Roe World' (2023) *Florida Law Review* (forthcoming).

⁶⁹ See, eg, Amazon.com.au, 'Interest-Based Ads' (Web Page) <https://www.amazon.com/gp/aw/help?id=201308670#:~:text=Advertising%20Preferences>

⁷⁰ Attorney-General's Department, 'Privacy Act Review: Report 2022', 213.

⁷¹ See, eg, 'In the Matter of Betterhelp, Inc.' (United States of America Before the Federal Trade Commission, 2023169); BetterHelp, 'BetterHelp's Response to the Recent FTC Settlement' (Press Release) <https://www.betterhelp.com/betterhelp-response-to-the-recent-ftc-settlement/>

⁷² What to Expect Privacy Policy (updated 10 October 2022).

⁷³ Pregnancy+ and Baby+ Privacy Notice (updated 9 May 2022).

⁷⁴ Period Calendar – Abishkking Ltd Privacy Policy (updated 13 September 2022).

⁷⁵ Attorney-General's Department, 'Privacy Act Review: Report 2022', 116-120.

⁷⁶ APP 11.2.

⁷⁷ The exception is that the six-month retention period will start again "if the same user subsequently visits or interacts with an ad, email, the Services or a Channel". Since a "Channel" is defined to mean "What to Expect" services as well as "context and ads on third party websites, applications, platforms and other media channels", the six months would effectively restart whenever a consumer uses the Internet.

⁷⁸ Ovia Health Apps Privacy Policy (updated 21 December 2022).

⁷⁹ See Table 3.

⁸⁰ Attorney-General's Department, 'Privacy Act Review: Report 2022', 221-229.