Periods Tracked

Gemma Watson: gemmamwatson@gmail.com

Menstrual tracking should be a public health service rather than a commercial product.

Researchers from the Minderoo Centre for Technology and Democracy report that users vastly underestimate the commercial value of the data they log in these app.

Information about pregnancy or fertility intentions can be over 200 times more valuable to advertisers than basic demographic data such as age or location.

On average those surveyed expected the data to be worth 15x more greatly underestimating how valuable this data is

Awareness Creates Change

In 2019, Privacy International released a report that showed 62% of the apps they tested were sharing sensitive data on their users' health to Facebook.
6 years later, in 2025, they repeated their investigation, reviewing the 10 popular apps and found that they had all changed their practices, and **0 of the apps still share sensitive data without the users' permission.**
Showing how scrutiny from researchers and greater awareness amongst users has pushed these technologies towards higher privacy standards

Not Settling for Better

Standards for menstrual tracking apps have improved, but there is still considerable work to be done. In May 2025, the observer reported the National Police Chiefs' Council has issued guidance encouraging officers to search women's homes and seize phones following sudden pregnancy loss in some cases, **including looking for evidence such as menstrual-cycle or fertility-tracking apps to "establish a woman's knowledge and intention in relation to the pregnancy".**
Research indicates users are unclear about how their data may be shared, analysed, or accessed by third parties. **Only 1 of the top 8 Cycle tracking applications (CTAs) (Flo)** explicitly informs users in its privacy policy that health data may be handed over to law enforcement if requested during an investigation.

78% of those survayed where not aware that data they logged could be requested by law inforcment

New risks

Artificial intelligence is beginning to be integrated into cycle tracking applications to create features such as chatbots that can generate insight about an individual's health. This is a useful feature for many users, but it also increases the importance of clear policy and strong privacy protection. Sensitive reproductive health data could be exposed or shared with third parties if safeguards are not carefully implemented.

A Goverment Funded Alternative

Developing an NHS-run menstrual cycle tracking app could provide a trusted alternative to profit driven private platforms. As part of the UK public healthcare system, such an app would be subject to UK GDPR and NHS data governance frameworks, Creating more accountability and reducing the risk of data misuse. The app also has the potential to be a trusted platform to provide safe and accurate education on menstrual and sexual health.

Data For Reserch

A data set that uses anonymised data collected from an NHS-developed app would be a valuable resource for advancing understanding of menstrual health and reproductive health conditions.

Design Principles

Data Minimalisation

Data should only be collected where it is strictly necessary for the app's core functionality. Limiting data collection reduces exposure: data that is not collected cannot be misused or breached.

Local Storage

Providing users with the option to store data locally on their device increases user control and reduces reliance on centralised databases, thereby lowering the risk of data breaches.

Transparent Design

Privacy risks and data practices should be clearly communicated within the app. Users should be explicitly informed about the potential risks of logging sensitive data and provided with straightforward options to access and delete their data.

0% of those surveyed said they read the privacy policy of the app they used In full, 71% said they have never read it.

Limit 3rd Party Integration

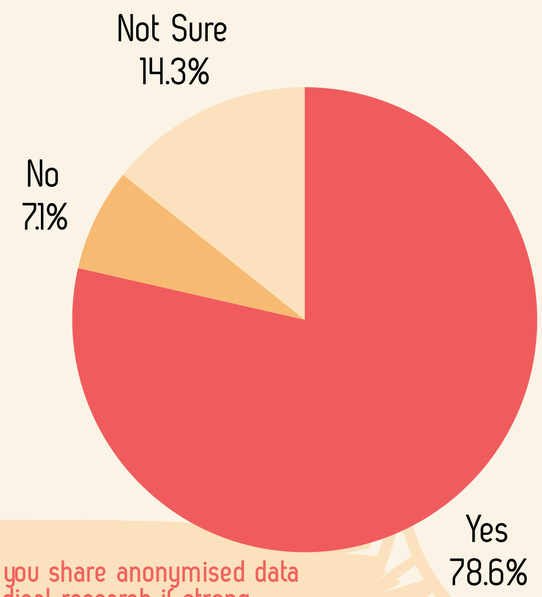
Many apps include small pieces of software from other companies, known as third-party software development kits (SDKs), for analytics, advertising, or crash reporting. These tools can collect information about a user's device or link activity across apps, creating more ways personal data could be exposed. They also create additional data flows beyond the app. Using fewer of these third-party tools and carefully auditing them is important to make a secure app

Clear Policys

Privacy policies should be easy to find and understand. They should clearly explain what data is collected, why it is needed, how it will be used, and how users can access, manage, or delete their personal information.

Storing Data Off Device Safely

Giving users the option to store data externally has the benefit of preventing data loss and adds convenience for users who can sync their data across multiple devices. Pseudonymisation is a technique that replaces identifying information (such as names or phone numbers) with codes or "pseudonyms" that refer to keys in a separate data set. It reduces the risk of storing data off-device by separating identifying data from the main dataset, reducing the ability to directly link data to an individual. This makes cloud-stored data safer by limiting the impact of breaches or unauthorised access..



Methods

In the process of collecting data for this poster, users of CTA were surveyed. The survey aimed to collect data on how aware users were of how their data was stored and shared. The design and privacy policies of the top 8 most downloaded apps from the Google Play Store. These apps included: Flo, Period Tracker by Simple Design, Maya by Plackal Tech, Period Tracker by GP Apps, WomanLog, Wocute, Stardust

Sources And More Information on the topics of this poster

University of St Andrews