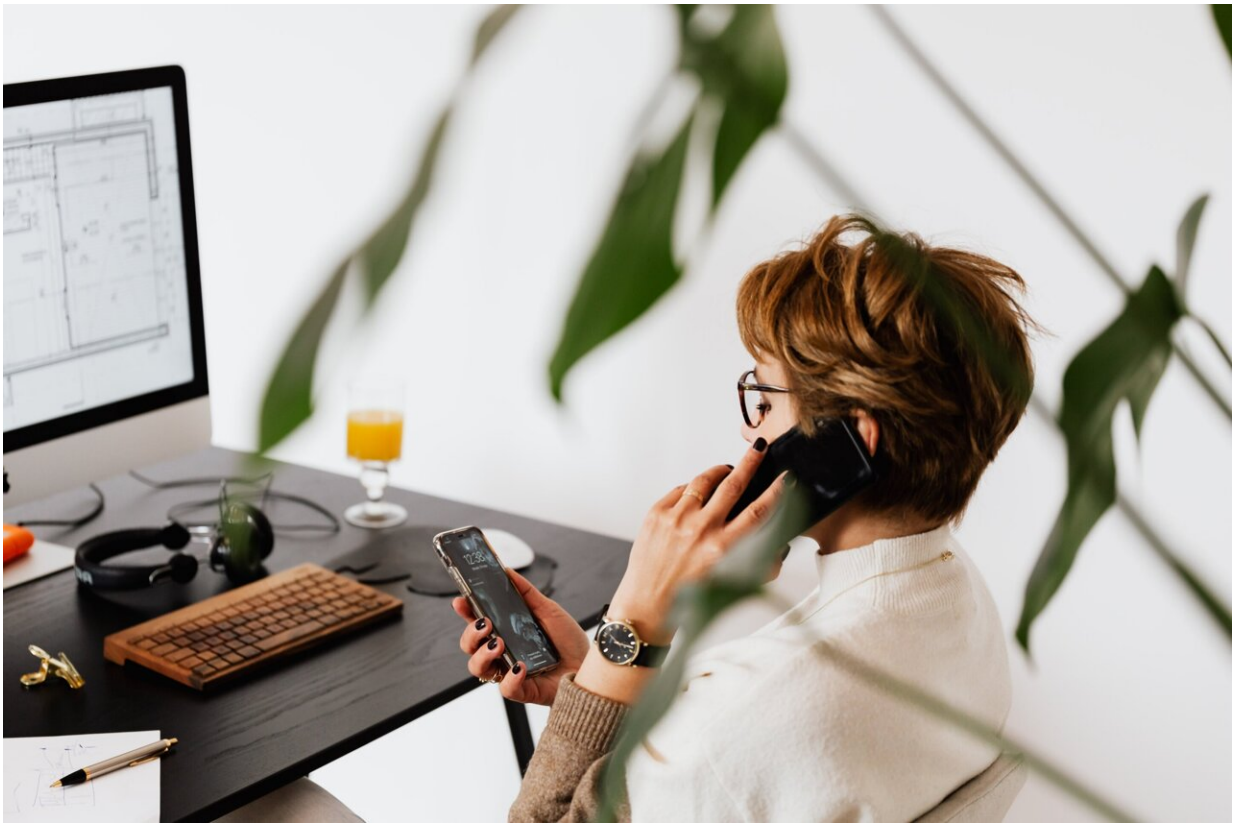
Female health apps misuse highly sensitive data, study finds

May 13 2024



Credit: Karolina Grabowska from Pexels

Apps designed for female health monitoring are exposing users to unnecessary privacy and safety risks through their poor data handling practices, according to new research from King's College London and

University College London (UCL).

In the most extensive evaluation of the privacy practices of female health apps to date, researchers found apps that handle medical and fertility data are coercing users into entering sensitive information that could put them at risk.

Following an analysis of the privacy policies and data safety labels of 20 of the most popular female health apps available in the UK and U.S. Google Play Stores—which are used by hundreds of millions of people—the study revealed that in many instances, user data could be subject to access from law enforcement or security authorities.

Only one app that the researchers reviewed explicitly addressed the sensitivity of menstrual data with regard to law enforcement in their privacy policies and made efforts to safeguard users against legal threats.

By contrast, many of the pregnancy-tracking apps had a requirement for users to indicate whether they have previously miscarried or had an abortion, and some apps lacked data deletion functions, or made it difficult to remove data once entered.

Experts warn this combination of poor data management practices could pose serious physical safety risks for users in countries where abortion is a criminal offense.

The research is being presented at the ACM Conference on Human Factors in Computing Systems (CHI) 2024, which takes place from 11–16 May 2024.

Lead investigator Dr. Ruba Abu-Salma, King's College London, said, "Female health apps collect sensitive data about users' menstrual cycle, sex lives, and pregnancy status, as well as personally identifiable

information such as names and email addresses.

"Requiring users to disclose sensitive or potentially criminalizing information as a pre-condition to deleting data is an extremely poor privacy practice with dire safety implications. It removes any form of meaningful consent offered to users.

"The consequences of leaking sensitive data like this could result in workplace monitoring and discrimination, health insurance discrimination, intimate partner violence, and criminal blackmail; all of which are risks which intersect with gendered forms of oppression, particularly in countries like the U.S. where abortion is illegal in 14 states."

The study, which looked at well-known apps including Flo and Clue, revealed stark contradictions between privacy policy wording and in-app features, as well as flawed user consent mechanisms, and covert gathering of sensitive data with rife third-party sharing.

Key findings included:

- 35% of the apps claimed not to share personal data with third parties in their data safety sections but contradicted this statement in their privacy policies by describing some level of third-party sharing.
- 50% provided explicit assurance that users' health data would not be shared with advertisers but were ambiguous about whether this also included data collected through using the app.
- 45% of privacy policies outlined a lack of responsibility for the practices of any third parties, despite also claiming to vet them.

Many of the apps in the study were also found to link users' sexual and reproductive data to their Google searches or website visits, posing, as

researchers warn, a risk of de-anonymization for the user and could also lead to assumptions about their fertility status.

Lisa Malki, first author on the paper and former research assistant at King's College London (now a Ph.D. student at UCL), said, "There is a tendency by app developers to treat period and fertility data as 'another piece of data' as opposed to uniquely sensitive data which has the potential to stigmatize or criminalize users. Increasingly risky political climates warrant a greater degree of stewardship over the safety of users, and innovation around how we might overcome the dominant model of 'notice and consent' which currently places a disproportionate privacy burden on users.

"It is vital that developers start to acknowledge unique privacy and safety risks to users and adopt practices which promote a humanistic and safety-conscious approach to developing health technologies."

Co-author Dr. Mark Warner, UCL, added, "It's important to remember how important these apps are in helping women manage different aspects of their health, and so asking them to delete these apps is not a responsible solution. The responsibility is on app developers to ensure they are designing these apps in a way that considers and respects the unique sensitivities of both the data being directly collected from users, and the data being generated through inferences made from the data."

To help developers improve privacy policies and practices of female health apps, the researchers have developed a resource that can be adapted and used to manually and automatically evaluate female health app privacy policies in future work. They are also calling for critical discussions on how these types of apps—including other wider categories of health apps including fitness and mental health apps—look after sensitive data.

The study was led by Dr. Ruba Abu-Salma, Lisa Malki, and Ina Kaleva from the Department of Informatics at King's College London, alongside Dr. Mark Warner and Dr. Dilisha Patel from UCL.

More information: Lisa Mekioussa Malki et al, Exploring Privacy Practices of Female mHealth Apps in a Post-Roe World, *Proceedings of the CHI Conference on Human Factors in Computing Systems* (2024). DOI: 10.1145/3613904.3642521 , dl.acm.org/doi/10.1145/3613904.3642521