Research exposes security, privacy and safety issues in female technology apps used to track fertility, monthly cycles

March 6 2024

Credit: Pixabay/CC0 Public Domain

Experts at Royal Holloway, University of London, Newcastle University, University of London, and ETH Zurich have identified significant security, privacy, and safety issues surrounding FemTech, which can pose a potential threat to users.

These threats include the apps accessing users' personal contacts, cameras, microphones, location, and other personal data (e.g., medical scans), as well as system settings and other accounts that expose security and privacy risks.

These apps and IoT (Internet of Things) devices collect a wide range of data about users, their relatives (children, partners, family), their bodies, and their environments via embedded sensors.

The research showed that such practices can reveal very sensitive and intimate information about users (such as gender, fertility, and medical data) to third parties.

FemTech is a term applied to the collection of digital technologies focused on women's health and well-being. FemTech includes applications, software, and wearable devices and can range from mobile period apps and fertility-tracking wearables to IVF services.

The authors are calling on policymakers to explicitly acknowledge and accommodate the risks of these technologies in the relevant regulations by presenting the findings in the journal *Frontiers in the Internet of Things* and Symposium on Usable Privacy and Security Workshop.

The market is estimated to reach more than $75 billion by 2025. The devices and apps reviewed in this study include a breast smart pump, cycle, and fertility trackers (such as bracelets and rings), a smart bottle, Kegel trainers, sex toys, menopause management solutions, a digital pill organizer, and general health trackers.

The research team reviewed the existing regulations related to FemTech in the UK, EU, and Switzerland to identify gaps in regulations, compliance practices of the industry, and enforcement by running experiments on a range of FemTech smart devices, apps, and websites.

Their analysis of FemTech-related regulations shows they are inadequate in addressing the risks associated with these technologies. The EU and UK medical devices regulations don't currently have any references to FemTech data and user protection. The GDPR and Swiss FADP have references to sensitive and special category data, which overlap with FemTech data. However, the industry practices include many non-compliant practices in data collection and sharing.

The study also focused on industry non-compliance. The team identified a range of inappropriate security and privacy practices in a subset of FemTech systems. The research shows that these systems do not brand as medical devices, do not present valid consent do not give extra protection to sensitive data, and track users without consent.

The authors show that, not only is such intimate data collected by FemTech systems, but also this data is processed and sold to third parties.

The findings have exposed a lack of research and guidelines for developing cyber-secure, privacy-preserving, and safe products.

Dr. Maryam Mehrnezhad, lead author of the research and Senior Lecturer at Royal Holloway, said, "We have identified multiple threat actors interested in FemTech data such as fertility and sex information."

"We have been conducting security and privacy research on this topic since 2019. Apart from our system studies, our user studies also highlight that end-users are indeed concerned about their intimate and sensitive data being handled by FemTech products."

"We constantly share our research results with the industry and related regulatory bodies, such as the Information Commissioner's Office. We hope to see better collaborative efforts across the stakeholders to enable

the citizens to use FemTech solutions to improve the quality of their lives without any risk and fear."

Professor Mike Catt of Newcastle University, one of the study authors, added, "We urge regulatory bodies to update and strengthen guidelines to ensure the development and use of secure, private, and safe FemTech products."

"Many of the apps surveyed access mobile and device resources, too. Some of these permissions are marked as dangerous, according to Google's protection levels. Such access potentially exposes contacts, cameras, microphones, location, and other personal data."

"Some specific permissions, such as access to system Settings and other Accounts on the device, also impose security and privacy risks. Access to sensors on the mobile phone can also be used to break user privacy. Users deserve better protection, especially where this relates to sensitive personal health and gender data."

More information: Maryam Mehrnezhad et al, Mind the FemTech Gap: Regulation Failings and Exploitative Systems, *Frontiers in the Internet of Things* (2024). DOI: 10.3389/friot.2024.1296599. www.frontiersin.org/articles/1 … 024.1296599/abstract

Provided by Royal Holloway, University of London