January 2025

REPHRAIN
Protecting citizens online

Privacy risks in female-centred technology (FemTech): enhanced regulatory framework needed to protect women's online privacy and security

Dr Jennifer Pybus (York University), Dr Mark Coté (King's College London)

About the research

FemTech – a portmanteau for 'female technology' – represents different apps, devices and sensors that aim to improve women's health. Over the past few years, FemTech has undergone rapid growth, catalysed by its promise to provide women with more agency over their own health and to close the 'gender data gap', the gendered disparity in data collection and analysis which overlooks women's experiences and specific health needs. Yet the expansion of this marketplace, which is now valued at US $60 billion, raises questions about how to regulate the health data these technologies collect, including intimate details about a woman's menstrual cycle, sexual activity, moods, or menopause symptoms.

Many FemTech apps rely on third-party companies to support their functionality, which can sometimes lead to the sharing of sensitive health data without clear transparency. This can include data being passed between the app and other companies, raising concerns about women's privacy and security.

To investigate how women's health data within FemTech apps is shared with third parties, our research, funded by the Social Science and Humanities Research Council (SSHRC) in Canada and REPHRAIN in the UK, analysed the 14 most downloaded menopause Android applications from the Google Play Store in the UK, EU, US and Canada. After examining what data these apps and third parties access, we compared our findings with the apps' privacy policies and data safety agreements – the two key documents that help users make an informed decision about whether to download an app and set up a profile.

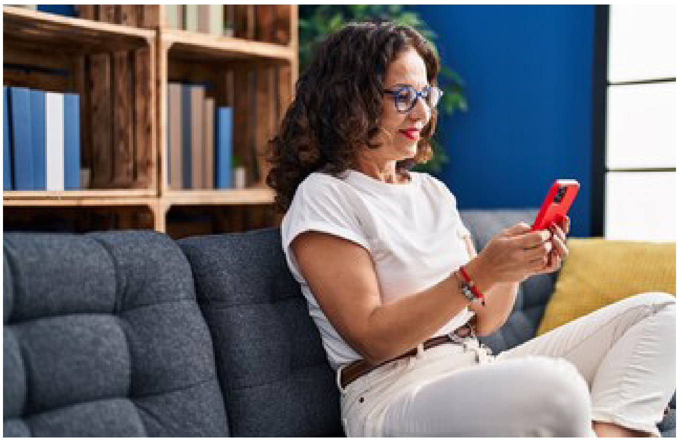

Image credit: Krakenimages.com via Adobe Stock

Policy recommendations

Enhance regulatory protection for health data

Health data collected by FemTech apps should be explicitly included in privacy legislation and classified as high-risk under GDPR. A comprehensive regulatory framework should mandate privacy-by-design principles for all FemTech apps, ensuring they proactively safeguard user data. This could involve requiring apps to conduct Data Protection Impact Assessments to identify and mitigate privacy risks before and during their operation.

Enhanced regulatory protection is especially important given the potential integration of FemTech into healthcare delivery (as noted in DHSC's 2022 report on Women's Healthcare Strategy for England).

Introduce regular audit and compliance checks

To ensure that FemTech apps are complying with GDPR laws and Google Play Store policies, they should be regularly audited, facing penalties or suspension from the app store if found to be violating them.

Enhance transparency to enable informed decisions

Users should be able to easily understand how different apps handle their personal and health data. Therefore, FemTech apps should be required to disclose all data-sharing practices with third parties in a clear and understandable way. The ICO could enforce standardised data-sharing disclosures.

Similarly, the Google Play Store should be held more accountable in reinforcing consistency between apps' data safety agreements and privacy policies to ensure users are informed when deciding to use an app.

Enable greater user agency

FemTech apps should be mandated to require opt-in consent for data-sharing practices beyond essential services. Users should be provided with a clear option to withdraw consent to data sharing and delete their health data at any time.

Key findings

Advertising

Eight apps had Advertising Identifiers (AdIDs) automatically enabled from Google and one app had AdIDs automatically enabled from both Google and Meta. This means that unique identifiers are being assigned to a user's device and are active by default, allowing applications and advertisers to track user behaviour for targeted advertising purposes. This directly conflicts with GDPR regulations.

Sharing health data

Eight of the 14 apps were sharing app 'event' data with third parties without a clear explanation of what this means to users. App event data captures user activity in an app, such as clicking buttons, watching videos, or making purchases.

However, in FemTech apps, it may also include sensitive health metrics like period tracking, mood logs, or medication use. Developers can use this data to understand app usage, but it can be leveraged for monetisation and targeted advertisements.

Inconsistent data governance tools

Our cross-referencing of the menopause apps with the Google Play Store's data safety agreements and privacy policies revealed inconsistencies. Four apps claimed to access, but not share, app event data in their data safety agreement but then reported sharing it with third parties in their privacy policy. This is grossly misleading, especially since many users do not read privacy policies.

Collecting and sharing other data

It was often only in the apps' privacy policies, not data safety agreements, that apps reported that users' addresses, phone numbers and purchase histories would be shared with third parties.

In addition, almost every app was sharing email addresses, user IDs, device identifiers and IP addresses. This is not required for app functionality, and therefore violates GDPR.

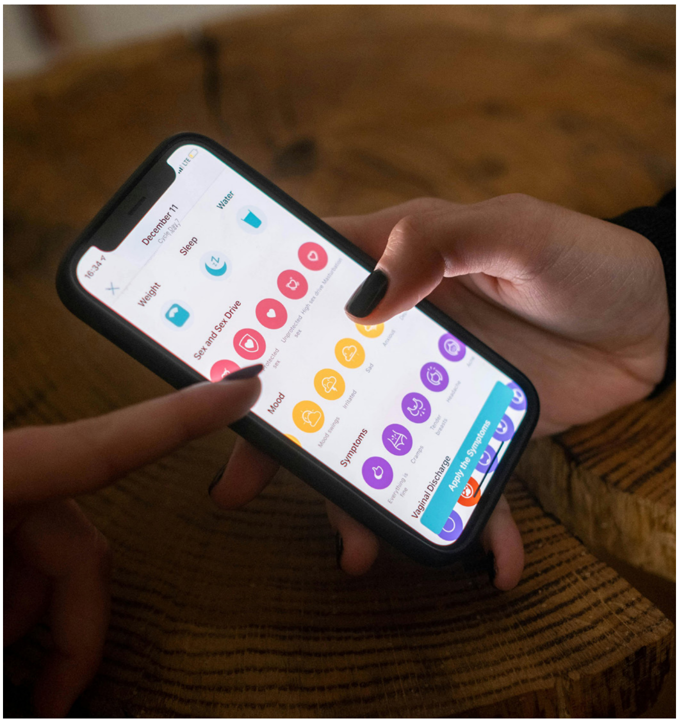

Image credit: cottonbro studio via Pexels.

REPHRAIN, led by the University of Bristol and partnered with University College London, King's College London, the University of Edinburgh, and the University of Bath, unites experts across disciplines such as Computer Science, Law, Psychology, and Public Policy to explore how to keep people safe online while enabling full participation in digital technologies. Announced by UKRI in October 2020, REPHRAIN now has over 100 experts from 23 UK institutions, working across 50+ research projects to build the UK's leading interdisciplinary community in this mission.

Further information

Pybus, J. and Mir, M. (2024) 'Tracking Menopause: An SDK Data Audit for Intimate Infrastructures of Datafication with ChatGPT4o'. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5054410.

Contact the researchers:

Dr Jennifer Pybus, Associate Professor, Canada Research Chair in Data, Democracy and AI, Department of Politics, York University – jpybus@yorku.ca
Dr Mark Coté, Reader in Data and Society, King's College London – markcote@kcl.ac.uk

YORK U UNIVERSITÉ UNIVERSITY

KING'S College LONDON