

## Insights

# WHAT IS FEMTECH AND HOW CAN IT MEET THE PRIVACY NEEDS OF ITS USERS?

Mar 08, 2024

## SUMMARY

In part one of our series "**FemTech: how this growing industry can build trust, protect privacy and redress healthcare inequity... one app at a time**", we take an introductory look at the industry, and offer some commercially-minded approaches to address users' privacy needs.

## WHAT IS FEMTECH?

Relatively speaking, female biology is complicated. So much so, that female subjects (of all species) tended to be excluded from pharmaceutical clinical trials until the early 1990s (and claims of under-representation persist). With more stages in their reproductive lifespan than men (think: menstruation, fertility, pregnancy, birth and menopause), it is small wonder that women are 75% more likely than men to use health apps - by 2021 over 50 million women worldwide are believed to have engaged with period tracker apps alone.

The term "*FemTech*" was coined to refer to a growing family of software, services and products that use technology tailored towards women's health and wellness needs. It includes fertility solutions, menstrual cycle tracking apps, as well as services which can support antenatal care, menopause and sexual health. It represents a rapidly growing market segment: the global FemTech market was estimated at approximately £41 billion in 2021 and is forecast to double in value by 2030.

## THE PRIVACY NEEDS OF USERS

Alongside the growing adoption of FemTech, there are elevated levels of concern over the use and security of information shared by users with providers, typically via apps. Onward-sharing of user data and possible "data leakage" is also coming under increased focus from regulators and consumer focus groups (we will cover this in our Part 2 article). In particular, in the context of greater scrutiny of online advertising, the interaction between app providers and the digital advertising eco-system accompanying FemTech needs careful consideration and transparency.

User trust is essential for the prosperity of the FemTech industry, and ‘trust’ is a fragile commodity in the online space.

Information shared by users with FemTech services can range from personal data (such as name, photo, location, age, weight, height) to special category personal data (e.g. diagnosed medical condition, prescribed medication, biometric data, state of mind, e.g. depression, sleep patterns, temperature, history of prior miscarriage, etc). This potentially gives the provider a highly detailed and sensitive data set which can, and is, used to customise or personalise the service or content (“*Trying to conceive? Then consider folic acid supplements*”), or to identify users as belonging to particular groups.

## THE TREND IN CUSTOMISATION AND PERSONALISATION

Enabling customisation or personalisation of the product/service offering, by its very nature, is dependent on the information held or inferred about the provider’s customer base. Users now tend to expect a degree of personalisation, on the understanding that their data will be used to drive more relevant recommendations and improve the experience. In the FemTech context, this might include recommended reading materials for a particular life stage or medical information about the early stages of pregnancy. Customised feeds based on profiling might include advertising content, links to content provided by other websites, downloads, other user generated content, written, audio or visual content. Profiling may also be used to suggest other users to ‘connect with’ or ‘follow’ if, for example, there is a community element to the service.

## A NEED FOR BALANCE

Regulators and customers alike will expect a clear balance to be struck between personalisation and the role of any third parties involved in facilitating it. The ICO’s [2023 consultation on period tracking apps](#) included the results of a poll, which revealed that, of the 1,000+ individuals surveyed, a third of these had used apps to track periods or fertility. Of those surveyed, transparency over how personal data was used (59%) and how secure it was (57%) were bigger concerns than cost (55%) and ease of use (55%) when choosing an app. It also found that over half of people who use such apps perceived an increase in baby or fertility-related adverts since signing up (which some found distressing).

The [Organisation for the Review of Care and Health Apps \(ORCHA\)](#) and the [Norwegian Consumer Council](#) each conducted reviews of a range of FemTech apps in 2020 and 2022 and expressed concerns about data sharing practices. [ORCHA’s 2022 review](#) indicates that more needs to be done on the compliance front, particularly as regards the sharing of personal data with third parties and the way in which users are invited to give consent for their personal information to be used. It found that consent to data sharing was commonly bundled within the overall terms of use for the app, which are often lengthy and rarely read in detail (unless you are a data privacy lawyer!).

While we understand the ICO's review (of around 11 providers of period and fertility tracking apps) did not indicate any serious compliance issues or evidence of harms, the ICO identified improvements all app developers could make, to ensure they are meeting all their obligations to be transparent with their users and to keep their data safe. The ICO issued four practical tips, focussed on (1) the need for transparency, (2) obtaining valid consents from users, (3) establishing the correct lawful basis for the processing of personal data and (4) accountability to users.

## KEY PRIVACY ISSUES

The key privacy issues for FemTech companies to consider include:

- Does the product/service offer clear and transparent choices to its users about how their data is used and shared with third parties, such as advertisers, data brokers, research institutions, or law enforcement agencies? Do users have a meaningful choice when they agree to sign up to use the product? 'Bundled' consent is unlikely to be valid consent under the UK GDPR/GDPR.
- Are there appropriately robust security measures in place to protect user data from unauthorised access, loss, or breach (which could expose users to identity theft, fraud, discrimination, or harassment)?
- When looking at ways of tailoring the user experience by offering bespoke, relevant content to a user, have you considered how to mitigate the potential harm or distress users might experience receiving unwanted or inappropriate targeted ads or messages based on personal data, such as pregnancy or fertility-related ads?
- Can users exercise their rights to access, delete, or correct their data, or to opt out of (or amend) their data collection and sharing preferences? Is it easy to toggle these choices over the course of the use of the app?
- Have the ethical and social implications of using FemTech in different cultural and legal contexts been adequately addressed? In particular, in jurisdictions where women's rights and freedoms may be restricted or are in a state of flux, does access to the app need to be geo-fenced to protect users e.g. accessing information about abortion or sexual health clinics?

Given the potential global user base and complex regulatory environment for these technologies, seeking appropriate legal and regulatory advice (including conducting privacy impact assessments and drafting appropriate user policies) at an early stage ensures your business is built on a strong foundation. Rapidly growing businesses will want to ensure that their governance and compliance posture meets the expectations of users, regulators and investors.

In the next part in this series, we will explore the UK and EU regulatory privacy landscapes and how they apply to FemTech sector. Our final instalment will examine future developments and best practices.

---

Your BCLP Data Privacy contacts: Kate Brimsted and Anna Blest

Meet the BCLP Healthcare team: Manuela Ampontuah, Virginie Brault-Scaillet, Laura Patao-Caminas, Flora Haidar, Jennifer Hutchens, Marcus Pearl, Seth Pearson, Geraldine Scali and Benjamin Wheeler.

## **RELATED PRACTICE AREAS**

- Data Privacy & Security
- Healthcare & Life Sciences
- Technology Transactions
- M&A & Corporate Finance

## MEET THE TEAM



### **Kate Brimsted**

London

[kate.brimsted@bclplaw.com](mailto:kate.brimsted@bclplaw.com)

[+44 \(0\) 20 3400 3207](tel:+442034003207)



### **Anna Blest**

London

[anna.blest@bclplaw.com](mailto:anna.blest@bclplaw.com)

[+44 \(0\) 20 3400 4475](tel:+442034004475)

---

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon ([kathrine.dixon@bclplaw.com](mailto:kathrine.dixon@bclplaw.com)) as the responsible attorney.