BCLP. Client Intelligent

Insights

NAVIGATING THE FEMTECH REGULATORY LANDSCAPE: BEST PRACTICE & FUTURE DEVELOPMENTS

Jul 19, 2024

The stakes are high for FemTech – as Benjamin Franklin noted: 'it takes many good deeds to build a good reputation and only one bad one to lose it.' As technology continues to outpace regulation in this sector, there is a pressing need for improved practices and standards. Since our last installment, a team at King's College London published research into the privacy practices of 20 popular female mHealth apps available in the US and UK Google Play Stores and highlighted certain practices of concern. These include inconsistencies across privacy policy content and privacy-related app features, poor consent collection and data deletion mechanisms, as well as the covert gathering of sensitive data. Given the privacy risks and challenges that this technology poses - heightened in the US by the 2022 overturning of the *Roe v. Wade* decision and with it the constitutional right to abortion - companies, users and regulators should adopt better practices now to enhance the protection of women using these health-empowering services. The benefits of doing so are not limited to the users of these apps. Building trust through implementing ethical behaviors could lead to a competitive advantage for developers in this marketplace (not least in attracting funding and further investment). Research suggests robust and transparent privacy protections correlates with better user experience and trust and can drive increased uptake amongst users.

We have distilled some best practice recommendations below.

EMBED PRIVACY BY DESIGN

- Design and develop FemTech products and services with users in mind from the outset and consult user groups as part of the data protection impact assessment (DPIA) process to identify and mitigate potential privacy risks and harms. Bear in mind the ICO's Age Appropriate Design Code also applies if children are likely to use your service (which may catch some adolescent users of period tracking apps), as this Code extends to all those under the age of 18. This exercise should include reviewing technical 'privacy' language used to ensure users are clearly informed about their rights. DPIAs should form part of the bedrock of the design process. All privacy settings should be set to their highest setting by default.

- Apply the principles of data minimisation, privacy by design and by default, and accountability, and ensure that only the necessary and relevant data is collected, processed, and stored, and that adequate security measures are in place to prevent unauthorized access, loss, or breach.
- Personal data should not be retained for longer than necessary for the purpose for which it was originally collected (however, to the extent the personal data can be truly anonymized, this restriction no longer applies). Be mindful of the current UK and EU regulatory focus on online choice architecture amid concerns about the ability of consumers to navigate and understand lengthy online terms and / or set and adjust their user preferences. US best practice guidance states that users should have easy access to review the data retention policy.

FACILITATE MEANINGFUL USER CHOICE FROM THE OUTSET: APPLY A USER-CENTRIC LENS

- Avoid processes which make it difficult for users to opt out of aspects of your service (whether on enrollment or subsequently during use of a product or service) or to identify to the user when supplying particular data is optional. Ensure users are informed about information being accessed automatically from a user's device, or where data is automatically imported when a user logs into an app from a social media platform.
- When considering the types of user profile you wish to build, consider if the collection and linking of data points across multiple platforms and websites risks creating sensitive inferences about users and whether this is permissible under data protection laws in the jurisdiction in which you are operating.
- Provide clear and fair information about the data usage and sharing practices, and the rights and choices of the users, using layered privacy notices (and potentially allowing granular consent options for advertising and analytics and tailoring of specific privacy preferences), graphical elements, and user-friendly interfaces. Avoid using generic or vague terms, such as "third parties", and directly name all the companies that have access to or analyse user data. The King's College research indicated that there are often inconsistencies between the information provided by app developers in the Google Play Store data safety form and details of information sharing set out in the privacy policy (with a number of apps which claimed in the data safety section not to share user personal data setting out some levels of sharing in privacy policies, including sharing user demographics with advertisers, transmitting health data to third party processors, and potentially disclosing personal data to law enforcement). Where a privacy policy covers multiple apps, ensure that it still contains details relevant to the specific data processing practices of the particular app.

EMPOWER USERS AND RESPECT LOCAL PREFERENCES

- Obtain valid and informed consent from the users or rely on another lawful basis for processing personal data and respecting the users' preferences and decisions. Avoid making the use of the service conditional on accepting tracking and sharing of personal data for further purposes, such as advertising, and avoid using dark patterns or nudging techniques to influence the users' choices (such as by bundling consents together and thereby obscuring key aspects of the terms of use).

- Enable users to exercise their rights to access, delete, correct, restrict, or object to the processing of their personal data, and to opt out of data collection and sharing, by providing easy and accessible mechanisms, such as email addresses, telephone numbers, or in-app settings. Interestingly, the King's College research flagged concerns about users who had opted to uninstall female mHealth apps in the wake of recent US developments, noting that it was not clear if this would protect users in the US from criminalization, as historical data may still be retained by developers. Mechanisms for both data deletion and portability are important enabling users: (i) by deleting to restrict sensitive data which may be held by the third-party developer; and (ii) to move their data to a new mHealth provider without losing access to historic data. There is also a need to ensure data deletion tools are clearly identifiable as well as enabling users to set restrictions on the processing of their personal data via easily accessible opt-out tools.

- Consider the ethical and social implications of use of digital health technologies in different cultural and legal contexts and consider the needs and vulnerabilities of the users. Ensure users understand where their data is stored and provide options for the users to change the location of data storage (or to always store data locally on the user's own device), to delete data permanently, or to use the service with discretion, in case of a threat to their safety or rights. Inform users of any rights that law enforcement may have in a particular jurisdiction to access their personal data. Consider if there are circumstances in which geofencing might be appropriate, to prevent inadvertent use of the app in jurisdictions where the legislative regime is in flux.

IMPLEMENT ROBUST CONTROLS, GOVERNANCE AND SECURITY MEASURES

- Ensure clear and auditable records of user consents obtained are retained. Details of the privacy policy should be available before the user enters their sensitive data. Consider addressing accessibility issues by creating visual summaries of privacy policies through a short form 'privacy label' to aid user comprehension of key terms (making sure the terms of this label conform to the detailed privacy policy).

- Implement strong security measures to protect sensitive health data, including encryption. Consider anonymizing or pseudonymising data where possible, especially if data is being held on servers rather than locally on users' devices.

- Conduct careful vetting of third parties that may receive data and form part of your digital ecosystem and ensure appropriate data processing agreements are in place. Explain your data processing policies to the third parties so they can comply.

STAKEHOLDER ENGAGEMENT AND HORIZON-SCANNING

- Engage proactively with the regulators and other stakeholders, such as civil society groups, academic institutions, lobbyists, nonprofits and industry associations, to share best practices, insights, and challenges, and to contribute to the development and implementation of privacy standards and regulations.

- Be mindful of the impact of the EU's Digital Services Act, which requires platform providers to ensure transparency of targeting parameters, mandates increased user control over targeting settings and will see an end to the targeting of advertisements on online platforms based on special category data (as well as an end to online advertisements targeted at children). This has been in force since 17 February 2024 and will significantly impact the digital advertising ecosystem. The US does not have an equivalent of the Digital Services Act, but many companies that are regulated under the Digital Services Act are headquartered in the US. Some of these major companies have stated they will make certain changes that will only apply to EU citizens.

The future of FemTech is likely to see more innovation and growth, as well as more regulation and scrutiny, as the demand and supply of women's health and wellness products and services increase, and as the awareness and expectations of the users and the regulators evolve. Companies and regulators operating in this sector must work together to ensure that they can deliver FemTech's benefits and reach its potential, while also respecting and protecting the privacy and dignity of women. Whilst women's health has been notoriously underserved in the past and it is clear the FemTech sector deserves and needs to grow and thrive, it is a sector that is ill-suited to a 'move fast and break things' mentality. There is a risk that high profile issues with data privacy could stifle the investment in innovation that is so keenly needed to empower women seeking to play a more active role in manging their health and fertility.

This checklist for developers aims to enhance the protection and empowerment of women's health and data in the female mHealth space.

CHECKLIST FOR DEVELOPERS

- **User-Centric Design**: Start with your users in mind and consult user groups to mitigate privacy risks and respond to their concerns.

- **Data Principles**: Apply data minimisation, privacy by design, and accountability principles.

- **Clear Information**: Provide transparent data usage and sharing information using user-friendly interfaces.
- **Consent and Choice**: Obtain valid consent and respect users' decisions without using dark patterns.
- **Security = Safety**: High levels of security are essential. Diligence needs to extend to all third parties you use to provide the service that could access user data.
- **User Rights**: Enable users to access, delete, or restrict their personal data easily.
- **Cultural and Legal Considerations**: Be mindful of the ethical implications in different contexts.
- **Regulatory Engagement**: Proactively engage with regulators and stakeholders setting privacy standards.
- **EU Digital Services Act Compliance**: Be ready to adhere to the new transparency and targeting requirements, if serving EU users.

RELATED ARTICLES

What is Femtech and how can it meet the privacy needs of its users?

We take an introductory look at the industry, and offer some commercially-minded approaches to address users' privacy needs.

Navigating the Femtech regulatory landscape: which rules apply and what are the enforcement priorities?

Security, scale or functionality – pick two. This computer science principle coined by the late Professor Anderson is particularly relevant to the FemTech industry.

RELATED CAPABILITIES

- Healthcare & Life Sciences
- Technology Transactions

MEET THE TEAM

Anna Blest

London
anna.blest@bclplaw.com
+44 (0) 20 3400 4475
