Exploring Privacy Practices of Female mHealth Apps in a Post-Roe World

Lisa Mekioussa Malki
lisa@malkihome.co.uk
King's College London
UK

Ina Kaleva
ina.kaleva@kcl.ac.uk
King's College London
UK

Dilisha Patel
dilisha.patel@ucl.ac.uk
University College London
UK

Mark Warner
mark.warner@ucl.ac.uk
University College London
UK

Ruba Abu-Salma
ruba.abu-salma@kcl.ac.uk
King's College London
UK

ABSTRACT

Mobile apps which support women's health have developed rapidly alongside the increasing de-stigmatisation of female reproductive wellbeing. However, the ubiquity of these apps has advanced the practice of intimate surveillance and the commodification of sensitive user data. While the overturning of Roe v. Wade has prompted reflection on the privacy and safety implications of female mobile health (mHealth) apps, the privacy practices of these apps have yet to be thoroughly examined in a post-Roe world. We investigated the privacy practices of 20 popular female mHealth apps, combining a thematic analysis of Data safety sections and privacy policies with a privacy-focused usability inspection. Our findings revealed problematic practices, including inconsistencies across privacy policy content and privacy-related app features, flawed consent and data deletion mechanisms, and covert gathering of sensitive data. We present recommendations for improving privacy practices, and call for a dedicated focus not only on user privacy, but also safety.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**.

KEYWORDS

Digital health, mobile health, FemTech, women's health, privacy, safety

ACM Reference Format:
Lisa Mekioussa Malki, Ina Kaleva, Dilisha Patel, Mark Warner, and Ruba Abu-Salma. 2024. Exploring Privacy Practices of Female mHealth Apps in a Post-Roe World. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3613904.3642521

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642521

1 INTRODUCTION

Female mobile health (mHealth) apps provide innovative opportunities for the management of women's health by offering period, fertility, and sexual activity tracking and predictive services [24]. They are a subgroup of a broader Female Technology (FemTech) industry that uses technology to support health issues in women and those who have female reproductive capabilities.[1] Female mHealth apps have unlocked novel opportunities for de-stigmatisation of the reproductive body, and improved healthcare access and affordability [26, 55, 95]. Existing research has explored how the design of these apps could be improved by addressing menstrual literacy [59, 95] and gender inclusivity [89, 93].

Privacy has recently emerged as another crucial dimension of analysis, predicated by widespread concerns about the misuse and misappropriation of user data by app developers [3, 64]. Female mHealth apps collect sensitive data about users' menstrual cycles, sex lives, and physiological wellbeing, as well as personally identifiable information (PII) such as names and email addresses [2]. A lack of adequate management of personal data has advanced the practice of *intimate surveillance*, in which sensitive data is commercialised at the expense of user privacy [56]. These discussions have grown in urgency following the overturning of Roe v. Wade in 2022, which ended the federal right to abortion in the United States (US) [18]. The event has catalysed widespread fears of increased governmental surveillance and criminalisation of women seeking abortions [22] both in the US and in the United Kingdom (UK), where abortion remains a criminal offence unless authorised by two physicians and performed within a legal time limit [13, 94]. Illustrating this, a recent poll by the Information Comissioner's Office (ICO) found that over half of women in the UK are concerned about the privacy and security of period-tracking apps in the wake of Roe v. Wade [46].

The overturning of Roe v. Wade has resounded on a global level, marking a shift in how female mHealth app users navigate sharing reproductive health data [22]. While the response of some users has been to delete these apps [32], they continue to play a crucial role in health management for many [95]. Furthermore, it is unclear as to whether uninstalling female mHealth apps actually protects

[1] We use the terms *FemTech* and *female mHealth apps* to remain consistent with how these technologies are described in industry [3]. We refer to FemTech users as women to remain consistent with how participants have been described in previous works. However, we acknowledge that some users of FemTech may not identify as women or as female but are included in our work as users of FemTech.

users from criminalisation, since historical data may still be retained by developers [41]. While there is evidence that developers have altered their apps to address this changing legal landscape [40, 88], the privacy practices of female mHealth apps in a post-Roe world remain largely unexamined. The overarching aim of our study, therefore, was to conduct an exploratory investigation of the privacy practices of popular female mHealth apps (as communicated through Data safety sections,[2] privacy policies, and app interfaces), and to explore implications of these practices for users in a post-Roe world. We address the following research questions:

RQ1. What are the privacy practices of female mHealth apps with respect to data collection, storage, sharing, deletion, and safeguarding as declared in Data safety sections and privacy policies?

RQ2. What in-app privacy features and mechanisms are available to female mHealth app users (e.g., data deletion, data portability, and consent/opting out), and how usable and useful are these features and mechanisms?

RQ3. Do inconsistencies exist between the privacy practices declared in Data safety sections and privacy policies, and actual in-app privacy features and mechanisms? If so, what are these inconsistencies, and could they negatively impact user safety following the overturning of Roe v. Wade?

To address our research questions, we conducted a thematic analysis of the Data safety sections and privacy policies of 20 popular female mHealth apps on the US and UK Google Play Stores, followed by a rigorous privacy-focused usability inspection. We triangulated findings from the two procedures, to identify areas of disconnect between what is declared in Data safety sections and privacy policies, and app features. Our work is the first in the FemTech space to combine an analysis of Data safety sections and privacy policies with a usability inspection, and builds on prior work by uncovering a diverse set of practices related to data collection, sharing, and safeguarding, and identifying their privacy and safety implications in a post-Roe world. We also draw attention to data retention practices, as well as the privacy rights afforded to users, such as data deletion and portability; a currently overlooked aspect of FemTech privacy, but one with concrete implications for users attempting to protect themselves against criminalisation. While our findings address the unique privacy and safety implications of female mHealth apps in a post-Roe world, many of our recommendations are generalisable to other types of mHealth apps. By reflecting on how the most intimate types of data (e.g., fertility data [3, 64]) can be protected to better safeguard users in challenging legal environments, we carve a pathway for improving the privacy practices of mobile apps more widely, and champion universal design [31]. We make the following three key contributions:

(1) We present findings from an in-depth, mixed-methods analysis of female mHealth app privacy practices. We explore a breadth of practices related to data collection, storage, sharing, deletion, and safeguarding, as well as consent and opt-out mechanisms.
(2) We provide actionable design recommendations to improve upon the shortcomings identified in our analysis of female mHealth apps, and stimulate critical discussions around the need to consider user *safety* in the privacy practices of mobile apps more broadly. Together, this constitutes an interdisciplinary blueprint for future work spanning HCI, user experience (UX) design, app development, and policy.
(3) Finally, we provide a codebook (see Table C.1 in Appendix C) developed through a combination of deductive and inductive thematic analysis of privacy policies. This codebook can be readily adapted to both manual and automated evaluations of female mHealth app privacy policies in future work.

[2]As per Google's developer guide [16], we capitalise the 'd' in Data when referring to Data safety sections and/or forms.

2 RELATED WORK

2.1 FemTech and Intimate Surveillance

FemTech is a category of software, apps, and diagnostics that cater to female health needs [80], including aspects of reproductive health [3]. Fertility- and menstrual-tracking apps continue to dominate the FemTech market, and are used by women worldwide for tracking periods [55], communicating with healthcare providers [17], and understanding their bodies [26, 34]. While many women use female mHealth apps to combat menstrual stigma and maintain dignity [55, 95], severe vulnerabilities and data breaches have been associated with FemTech companies [29, 83]. Consequences of FemTech data breaches could include workplace monitoring [14, 64], health insurance discrimination [19, 81], intimate partner violence [80], and criminal blackmail [3]; all of which are risks which intersect with gendered forms of oppression [64]. Shifts in the legal landscape surrounding abortion have exacerbated these concerns, both in the US following the overturning of Roe v. Wade [63] and in the UK, where abortion remains a criminal offence under the *1861 Offences Against the Person Act* [13, 18]. Therefore, the possibility that female mHealth app data may be used to criminalise at-risk individuals is a real threat that is felt by users internationally [22, 46, 55, 59].

Owing to the sensitivity and longitudinality of the data tracked by female mHealth apps, this can be considered a form of *intimate surveillance* [56], in which the personal lives of users are quantified over time and fashioned into a commercialisable resource; a practice which paradoxically, benefits male-dominated corporate interests at the expense of women's privacy [30]. Menstrual-tracking apps have been found to share excessive amounts of user data with third-party vendors, libraries, and Software Development Kits (SDKs) in past work [85], and while these acts are ostensibly performed with the consent of users, it is unlikely that they fully understand the ecosystems through which their information flows [56]—in contrast to the *Theory of Contextual Integrity (CI)*, which emphasises adherence to expected social (including privacy) and contextual norms in the gathering and transmission of data [71]. This creates a climate in which users become increasingly habituated or resigned to privacy practices which are invasive or excessive, and feel unable to meaningfully control their digital footprints in the face of reproductive threats [62, 68].

2.2 EU, UK, and US Data Privacy Laws

In the European Union (EU) and the UK, the use of data is regulated by the General Data Protection Regulation (GDPR), which places limitations on how personal data can be used by organisations,

and affords users rights over what data is collected, and how it is processed [36]. In a clear and intelligible fashion [28], those controlling personal data must provide information related to data retention policies, purposes and methods for data processing, and how data rights can be exercised. Rights under GDPR include the rights to access, rectification, and erasure of personal data, and the right to receive data in a structured and machine-readable format (data portability) [33]. Mechanisms for data deletion and portability have emerged as vitally important to users in a post-Roe world, since they allow users to sanitise their digital footprints in the case of sharing sensitive or criminalising data [95], and discontinue app use without losing access to historical data [30], respectively. However, data deletion mechanisms can be obscure and poorly designed, contributing to incorrect mental models of deletion operations among users of social media [82], the cloud [78], and popular operating systems [37]. Lastly, data subjects also have the right to restrict and object to the processing of their personal data under GDPR [99]—though mechanisms for opting out of web practices have been found to suffer from poor readability, poor usability, and ambiguity in outcomes [38, 39].

In the US, female mHealth apps are regulated by a "patchwork of federal and state laws" that cover different aspects of mHealth [81]. At a state level, laws have been enacted to cover different areas of digital privacy. The most significant is the California Consumer Privacy Act (CCPA), which offers protections and rights to Californian citizens [74]. The protections share many similarities with GDPR, including how personal data is defined, and subject rights to data access, portability, and deletion [100]. It also provides consumers with the rights to opt out of the sale of personal information [74], rectify data, and limit disclosure of sensitive personal information—a newly defined personal data type encapsulating sensitive characteristics such as precise geo-location and genetic data [53].

2.3 Privacy Practices of mHealth Apps

Designing strong and transparent privacy protections in mHealth apps correlates with better UX, trust, and more sustained uptake over time [23, 25]. However, existing studies have revealed alarming vulnerabilities associated with health apps across several domains, including fitness [66, 96], mental health [76], and COVID-19 tracking [6, 7, 42, 44, 47, 91]. For example, mental health apps are among the most widely researched in terms of privacy risks [72], and have been found to mine users' private chat transcripts for marketing purposes [69]. In the sphere of female sexual and reproductive health, studies have found that apps often harvest more data than needed for service provision [3, 85], and that this data often pertains to individuals other than the user, such as their family members or physicians [2]. While sensitive data is anonymised or aggregated by app developers, these safeguarding measures can be circumnavigated and users re-identified [72]. Female mHealth apps have also been found to contain 'socio-technical data traps' that make it deliberately difficult to limit data sharing during app use [64]. These data traps include not providing users with meaningful ways to opt out of privacy practices [30], lacking in-app data deletion operations [2], or making the privacy policy available only after the user has downloaded the app and entered sensitive data [2, 29, 64].

Transparency in how organisations collect and manage personal data is a requirement under GDPR and CCPA [33]. Privacy policies—textual documents which outline the purposes, legal basis, and uses of data collected by an app or a service—are the most common way that developers inform users of how their data is processed, and their rights with respect to this data [97]. However, user engagement with privacy policies is typically low, with studies reporting that users spend only a minute or so skimming the document [73], and that low readership is often linked to complexity in language and excessive length [45, 61, 79]. Existing work has used privacy policy analysis to understand the privacy practices of apps and websites, measure compliance with applicable laws and frameworks, and evaluate the quality and accuracy of privacy policies as a transparency mechanism [12, 65, 87, 98]. A small number of studies have reviewed the privacy policies of female mHealth apps specifically, finding that these apps either lack privacy policies altogether [2, 22, 64, 85], overuse technical terminology and jargon [3, 29, 85], or are generic and do not adequately address the unique privacy implications of fertility data [85].

A more recently introduced transparency practice is *privacy labelling*, which addresses the problem of lengthy and complex privacy policies by summarising the privacy practices of apps and websites in a short, 'nutrition label' format to aid visual comprehension [49]. The approach has since been adopted by the Apple App [5] and Google Play [16] Stores, which now require developers to submit high-level information about their app's privacy practices alongside a full privacy policy. While there is evidence that app users find privacy labels valuable and exhibit some intent to read them, prior work has also identified that users possess misunderstandings surrounding the authorship of privacy labels, and often overlook them when navigating app stores [102]. There are also concerns about the accuracy of privacy labels: a recent review of the Google Play Store's privacy labelling system ("Data safety sections") conducted by Mozilla [92] found that approximately 85% of apps exhibited discrepancies between the practices declared in the Data safety sections and the privacy policies of apps. Therefore, evaluating the accuracy of privacy labels is crucial to the FemTech app genre, since users may use the Data safety section to decide which apps pose less of a privacy and safety risk.

2.4 Summary

Overall, a body of work has explored the unique risks associated with FemTech [56, 80, 81], and evaluated the privacy practices of female mHealth apps using methods such as network analysis [20, 22, 27], checklist-based evaluations [2, 54], and reviewing privacy policies [3, 30, 85]. Most of these studies were conducted prior to the overturning of Roe v. Wade, though the event has led to shifts in how users, policymakers, and developers perceive the privacy of female mHealth apps worldwide [22], making our study timely and consequential. Furthermore, no studies to date have conducted an in-depth user interface (UI) inspection of female mHealth apps, with existing evaluations being limited to checking for pre-defined behaviours or privacy features such as consent notices [2, 54, 85]. We build on existing work in the usable privacy domain [39, 78, 82] by conducting a mixed-methods analysis of female mHealth app privacy practices that involved combining

a thematic analysis of privacy policies and Data safety sections with a rigorous UI inspection. We triangulated findings across our procedures, to identify inconsistencies and disconnects between the declared privacy practices and actual in-app privacy features offered to users. Thus, we contribute novel insights into how consent, data entry, data deletion, and data portability are implemented within these apps and offer actionable recommendations that can be applied to the FemTech app genre as well as the wider mHealth app ecosystem.

3 METHODS

Using a mixed-methods approach, we investigated the privacy practices of popular female mHealth apps available in the Google Play Store, since Android devices comprise over 70% of the world's mobile devices [90]. We thematically analysed the Data safety sections and privacy policies of 20 apps, and evaluated the app interfaces with a hybrid approach of two actively-used usability inspection methods in HCI research [43]: cognitive walkthrough [11] and heuristic evaluation [70]. We then triangulated our findings to identify areas of disconnect across the information declared by app developers in Data safety sections, the data practices described in privacy policies, and the app interfaces. After filling out a minimal risk registration form, our research was assessed by the Research Ethics Office at King's College London as not requiring a formal ethics review. In this section, we describe how we screened and selected apps, analysed their Data safety sections and privacy policies, and conducted our UI inspection.

3.1 App Screening and Selection

To select our sample, we performed keyword searches across the Google Play Store, the largest and most popular market for Android apps [2]. We included apps which were available in both the US and the UK Google Play Stores. We developed an initial set of search terms from a review of prior work [2, 17, 27, 85] and iteratively improved our terms by testing each with the Play Store search function and selecting terms that returned a wide variety of relevant apps. We used the following finalised set of terms for our search: *female health, women's health, reproductive health, fertility, ovulation, menstrual, menstruation, period, contraception, birth control, pregnancy, pregnant.* In March 2023, we developed and ran a Python script to automate the collection of all apps available in both the US and UK Google Play Stores that were returned by each search term. This returned a total of 184 unique apps.

We excluded apps which had zero user ratings (n=54), were not in English (n=3), had not been updated for over a year (n=35), and did not directly provide a service related to female reproductive health (n=29). We screened the remaining 63 apps based on their features, by inspecting screenshots provided on their Google Play pages and scanning the top 10-20 user reviews. As a result, we excluded apps that did not provide at least one tracking or predictive feature (n=7). We also excluded non-consumer-oriented apps, such as those aimed at healthcare professionals (n=4). This left a total of 52 eligible apps, including 40 period- and fertility-tracking apps and 12 pregnancy or baby apps. We ranked these apps based on the number of reviews they had received in the preceding 12 months, to ensure that apps that had been on Google Play for a shorter period of time but were rising in popularity were included [64], and selected the top 20 apps according to this criterion. We list the apps included in our analysis in Table A.1 (Appendix A).

3.2 Data Safety Section Analysis

Developers who have an app published on Google Play are required by Google to complete a "Data safety form" and provide a link to their app's privacy policy. This information is presented to users in a "Data safety section" which provides a concise summary of the types of data collected and/or shared by developers, the purposes for processing, whether user data is encrypted, and whether the developers give users an option to delete their data [16]. We manually extracted this information from the Data safety section of each app (see Table 1). Where available, the same information was extracted from the privacy policy text via a keyword search, facilitating comparison with the privacy policy.

3.3 Privacy Policy Analysis

We used a combination of deductive and inductive thematic analysis to analyse the app privacy policies, coding the policy text using MAXQDA. We began by drafting an initial codebook based on prior work examining privacy issues in FemTech [27, 85] and GDPR principles, particularly those related to user data rights (see §2.2) [33]. We selected GDPR as our initial guiding framework as it is a comprehensive and widely-used standard for evaluating the privacy practices of mobile apps [50], and has been discussed extensively in relation to FemTech products [64, 85].

Due to the technical complexity of privacy policy language and well-known challenges of accurately coding policy texts [65], our codebook underwent multiple rounds of iteration. The first author tested the initial codebook draft (developed deductively as described above) on a sample of five randomly selected policies and improved its coverage and structure, before sharing the revised version with the research team. Then, each author in the team (n=5) independently coded a different privacy policy and documented areas where existing codes failed to adequately capture the text. The team met to discuss revisions to the codebook, which included more coverage of concepts relating to the purposes of data collection, and sharing of data with third parties. Once these improvements were finalised, three authors conducted iterations of independently coding a set of 3-5 policies and meeting to discuss disagreements around coding and language interpretation [65], before refining the codebook. This process continued until code saturation was reached, and all authors were confident that the codebook was comprehensive and grounded in the data.

Then, all app policies were re-coded line-by-line by the first author in batches of five policies each, with all authors meeting at the end of each batch for discussions. Once all policies were coded, the data extracts assigned to each code were re-read and synthesised by the first author, yielding rich patterns and themes. We did not calculate inter-rater reliability (IRR).

Our codebook included the following key categories: (1) Policy Scope; (2) Policy Version; (3) User Data Types; (4) Data Collection Methods; (5) Purposes for Data Processing; (6) Data Storage/Retention; (7) Data Transfers; (8) Data Safeguarding Measures; (9) Regional Privacy Legislation; (10) User Privacy Rights; and (11)

Language and Readability. The codebook can be found in Table C.1 (Appendix C).[3]

3.4 Usability Inspection

To evaluate the usability of privacy-related app features, we conducted a rigorous UI inspection, combining cognitive walkthrough and heuristic evaluation. Cognitive walkthrough is a framework for evaluating how well a system supports the completion of specific tasks, and has been previously used to evaluate the usability of privacy features in popular mobile apps [1, 10]. Heuristic evaluation involves judging an interface against an established set of usability principles to identify design flaws [70]. We conducted a *heuristic walkthrough* [84]—a hybrid of the heuristic evaluation and cognitive walkthrough methods. Although there are advantages of involving users, evaluating interfaces without users is an effective method for identifying design issues, particularly when conducted by experienced evaluators [48]. Our protocol included a *preparation stage*, where we identified the target user and the tasks they would attempt with the app, followed by an *analysis stage*, in which we simulated using each app from the user's perspective and uncovered usability and privacy problems, guided by Nielsen's usability heuristics [70] and privacy-by-design principles [8, 15].

3.4.1 Preparation Stage. We began by defining the target user as a first-time or novice user of a female mHealth app, whose goal was to track aspects of their own sexual and reproductive health on an Android mobile device. Then, we identified relevant tasks around which to centre our evaluation. We installed all 20 apps on an Android mobile device, and systematically inspected all screens, buttons, and features. The key use cases and features of each app were documented, and condensed into a set of tasks and functionalities common to each app type, which included period, fertility, and pregnancy trackers. Tasks which involved accessing, inputting, or managing personal data were selected as the focal point of our analysis, as these tasks carried the clearest privacy implications for users.

3.4.2 Analysis Stage. Each app was independently analysed by the first and last authors. After wiping and re-installing the 20 apps to simulate first-time use, we walked through each task workflow step-by-step from the perspective of the user, reflecting on the language and visual layout of the UI. In particular, we considered whether the user would know how to proceed with each task, identify the correct actions, and correctly interpret system feedback regarding the outcome of these actions [84]. For each task, we also evaluated the interface against Nielsen's ten usability heuristics [70] and a set of privacy-by-design principles [8, 15] (see Tables B.1 and B.2 located in Appendix B). We documented any clear design problems alongside potential fixes or improvements. The independent findings of each author were collated and discussed within the research team using Miro, an online interactive collaboration tool [67]. Common design problems were identified through constant comparison, and aggregated into a set of privacy-related design practices and features.

[3]The MAXQDA file of the codebook can be shared upon request, so it can be used in future comparative research.

4 RESULTS

Our study investigated the privacy practices of female mHealth apps based on an in-depth analysis of the Data safety sections (see §4.1), privacy policies (see §4.2), and UIs (see §4.3) of 20 popular apps available in the US and UK Google Play Stores. The apps in our sample included period, fertility, and pregnancy trackers, and we identified a total of 18 unique app developers in our sample, with two developers creating more than one app: Amila developed apps #1 and #2, and Wachanga developed apps #19 and #20—corresponding app names and metadata can be located in Table A.1 in Appendix A. Half of the developers in our sample (9/18) exclusively developed FemTech-related products or services, such as period-, fertility-, and pregnancy-tracking apps. Seven developers made other health-related apps in addition to their female mHealth apps, such as weight loss and fitness apps and mental health trackers. The remaining two developers created generic categories of apps including games and file utilities.

4.1 Data Safety Section Analysis

We analysed the Data safety section of each app (see Table 1), and identified several inconsistencies between the information declared by developers in the Data safety sections and privacy policies across the apps in our sample.[4] Though broadly consistent in their descriptions of the types of data collected and purposes for data collection, the Data safety sections and privacy policies often differed with regards to *data sharing*, *data encryption*, and *data deletion* practices. All 8/20 apps which claimed in their Data safety sections to not share users' personal data described some level of third-party sharing in their privacy policies. This included sharing user demographics with advertisers, transmitting health data to third-party processors, and potentially disclosing personal data to law enforcement (see §4.2.5), which could lead to dire physical safety consequences for women in contexts where abortion care is criminalised [22]. Furthermore, out of the 19 apps that indicated that user data was encrypted in transit in their Data safety sections, eight made no mention of encryption in their privacy policies, and only four detailed the specific encryption method; e.g., Secure Socket Layer (SSL). Lastly, while 18/20 app Data safety sections stated that data could be deleted, two of these apps did not detail a procedure for deleting data in their privacy policies, or implement an in-app data deletion mechanism.

4.2 Privacy Policy Analysis

We identified a total of 19 unique privacy policies across the 20 apps, as two apps were created by the same developer and shared a generic privacy policy. A total of 18/20 apps had a privacy policy available in Google Play, and two had their policies located on their developer's website. By analysing all 19 privacy policies, we uncovered a breadth of practices related to data collection, use, storage, sharing, and safeguarding. We summarise these practices in Table 2.

4.2.1 Policy Length. The policies were on average 4,453.4 words long, though there was substantial variation in policy length (SD

[4]In Tables 1 and 2, and all screenshot captions, we refer to apps using their numerical IDs. The corresponding app names can be located in Table A.1 in Appendix A.

Table 1: App data practices declared in Google Play's Data safety sections.

	Data Collected							Data Shared							Security	
ID	App logs and interactions	Device data and IDs	Personally identifiable information	Health and fitness data	Location data	Multi-media data	Financial data	App logs and interactions	Device data and IDs	Personally identifiable information	Health and fitness data	Location data	Multi-media data	Financial data	Data Deletion	Data Encryption
1	x	x	-	-	x	-	-	x	x	-	-	x	-	-	x	x
2	x	x	-	-	x	-	-	x	x	-	-	x	-	-	x	x
3	x	x	x	x	-	-	-	-	-	-	-	-	-	-	x	x
4	x	x	x	x	x	x	-	x	x	x	x	x	x	-	x	x
5	x	x	x	x	x	-	-	-	-	-	-	-	-	-	x	x
6	x	x	x	x	-	-	-	-	-	-	-	-	-	-	x	x
7	x	x	x	x	-	x	-	-	x	-	-	-	-	-	x	x
8	x	x	x	x	x	-	-	x	x	x	-	x	-	-	x	x
9	x	x	x	x	-	-	-	-	-	-	-	-	-	-	x	x
10	x	x	x	x	-	x	x	-	-	x	-	-	-	-	x	-
11	-	-	-	-	-	-	-	x	x	x	-	x	-	x	x	x
12	x	x	x	x	x	x	-	-	x	-	-	x	-	-	x	x
13	x	x	x	x	x	x	x	x	x	x	-	-	-	x	x	x
14	-	-	-	-	-	-	-	-	x	-	-	x	-	-	-	x
15	x	x	x	-	x	-	-	-	-	-	-	-	-	-	x	x
16	x	x	x	x	-	-	-	-	-	-	-	-	-	-	x	x
17	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	x
18	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	x
19	x	x	x	x	x	-	-	x	x	x	x	x	-	-	x	x
20	x	x	x	x	-	x	-	x	x	x	x	x	-	-	x	x

= 2,636.3). The shortest app policy was just 300 words and only covered the cookie practices of the app developer's website. By contrast, the policies which gave the clearest descriptions of data handling practices were all at least 6,000 words long. However, long policies were not always more comprehensive and accurate. The longest app policy in our sample was over 10,000 words long, and contained several repeated sections and generic descriptions of data practices which applied to the website of the company that developed the app rather than the app itself.

4.2.2 Policy Scope. We analysed language relating to the scope of the privacy policies, and while some exclusively addressed the specific apps in our sample, other policies referred to all apps created by the app developer and other services, which included web portals, consultancy services, and advice networks. For instance, one privacy policy covered the mobile app, the developer's website, and *"any other services related to it."* Policies which covered multiple apps often did not refer to the functionalities of each app, which made it difficult to decipher app-specific data practices; for example, one privacy policy covered two different period trackers and a weight management app, however, it did not describe how data collection, processing, and management practices differed across the three apps.

4.2.3 Policy Updates. It is important that privacy policies are frequently updated, to stay relevant to the current data handling practices of the app and reflect changes in legal frameworks [12]. We found that 12/19 privacy policies had been updated within the last 12 months, 3/19 had not been updated since 2020, and four had no published date of last revision. Most policies (13/19) stated that the terms of the policy could change in the future, to reflect changes in services, legal obligations, or data management practices. While five indicated that the user would be notified of any material changes via email or in-app notifications, the rest placed the onus of determining whether the policy had changed on the user, instructing them to periodically check the developer's website or the privacy

Table 2: Key data practices declared in the privacy policy. An 'x' mark indicates the mention of a practice in the privacy policy, and '-' indicates that it was not mentioned.

ID	Policy Scope	Policy updated after Roe v. Wade (June'22)	Collects user input	Collects device resources and IDs	Collects cookies/tracking data	Service provision*	Research & development*	Personalisation*	Third-party advertising*	Mentions legal disclosure/subpoena	Mentions data retention policy	Mentions data safeguarding	Provides opt-out mechanism(s)	Provides data deletion via email request	Provides data deletion via device or app	Provides data portability
1	Single app	-	x	x	x	x	x	x	x	-	x	x	x	-	-	-
2	Single app	-	x	x	x	x	x	x	x	-	x	x	x	-	-	-
3	Single app	-	x	x	x	x	x	x	x	x	x	x	x	-	x	x
4	Single app	x	x	x	x	x	x	x	x	x	x	x	x	x	-	x
5	Single app	x	x	x	x	x	x	x	x	x	x	x	x	x	-	x
6	Single app	x	x	x	x	x	x	x	x	x	x	x	x	x	-	x
7	Single app	-	x	x	x	x	-	-	x	-	x	x	x	-	x	x
8	Multiple apps	-	x	x	x	x	x	x	x	-	-	x	-	x	-	-
9	Multiple apps	-	x	x	x	x	x	x	x	x	x	x	x	-	x	x
10	Multiple apps	x	x	x	x	x	x	x	x	x	x	x	-	x	-	x
11	Single app	-	x	x	x	x	x	x	x	x	x	x	-	x	-	-
12	Multiple apps	x	x	x	x	x	x	x	x	x	x	x	-	x	-	-
13	Single app	x	x	x	x	x	x	x	x	x	x	x	-	-	x	x
14	No relation	-	x	-	x	x	-	-	x	-	-	-	-	-	-	-
15	Multiple apps	-	x	x	x	x	x	x	x	x	x	x	x	-	x	x
16	Single app	x	x	x	x	x	x	x	x	-	-	x	-	x	-	x
17	Single app	x	x	x	x	x	x	x	x	x	x	x	-	-	x	x
18	Single app	x	x	x	x	x	x	x	x	x	x	x	x	-	-	-
19/20	Multiple apps	-	x	x	x	x	x	x	x	x	-	x	x	x	-	x

* Stated purpose for processing personal data.

policy's date of last revision. Continued use of the app was interpreted as consent to the revised policy, but no policy contained a summary of recent changes, and only one developer made previous versions available for viewing.

> *"Please check the revision date to determine if this Privacy Policy has been modified since you last reviewed it. Your continued use of any portion of the apps will constitute your acceptance of all such changes."*

4.2.4 Data Collection Methods. Methods by which apps collected user data included user input (e.g., a user entering the date of their last period), accessing device data and resources, importing data from third-party apps, and using cookies, data-logging, or other tracking technologies. Information accessed automatically from the user's device ranged from unique identifiers such as advertising IDs and IP/MAC addresses, to more general data relating to the operating system, device make, and resources such as camera, microphone, and GPS trackers. A total of 12/19 policies stated that apps automatically imported the user's name and profile data, activities, and contact lists from Google or Facebook when the user logged into the apps through these platforms. In 9/19 policies, data could also be imported from Apple HealthKit or Google Fit, including information about the user's sporting activities, weight, and heart rate. The data collected from fitness trackers can identify the user's exact location and their walking/exercise routes [96].

In addition to collecting app interaction logs, persistent cookies and third-party libraries were used to extensively profile users based on their demographics and web activities. These practices allowed data points from multiple platforms and websites to be linked, and sensitive inferences to be created about users, such as linking their sexual and reproductive data to their Google searches to "optimise" app content. Three policies explicitly stated that apps

did not respond to *Do Not Track (DNT)* signals, which allowed users to opt out of cross-browser tracking activities [101].

> *"Certain tracking technologies enable us to assign a unique identifier to you [...] we may combine your account data, Device data, cookies, location data, data collected during your interactions such as social media, websites, communications you click on or tap, location details and websites you visit [...]."*

4.2.5 Purposes for Data Collection and Processing. We identified four overarching purposes for collecting and processing user data: service provision and personalisation; research and development; advertising; and legal requirements.

Service Provision and Personalisation. All 19 policies stated that user data was processed to provide core app functionalities. Some simply stated that data was collected to *"provide a service"* or *"support and maintain the product"* without elaborating further (7/19), but most described specific use-cases (12/19) such as authentication, registration, and provision of tracking and predictive features. Third-party providers (e.g., Amazon Web Services) were often used to deliver specific parts of the service or provide technical functions. Essential app personalisation was cited as a purpose for processing data in 17/19 policies, and involved tailoring the app to the needs of individual users; e.g., customising articles, reminders, and suggestions for the user's current pregnancy trimester. As mentioned previously, apps combined interaction data (e.g., click paths, in-app searches), health and demographics, and location or device identifiers to create bespoke insights about users, and tailor apps accordingly.

> *"We rely on third-party infrastructure for the collection, transfer, storage, processing and fulfillment of our Services such as Amazon Web Services and Google Cloud Platform."*

Research and Development. All but two policies stated that user data was processed for research and app development activities, which included internal A/B testing, development of new features, detection of app crashes, and bug fixes (17/19). Some developers processed user data for clinical and scientific research, through sharing aggregated data with research institutions (3/19) or using data to recruit participants for clinical studies (1/19). Clinical research was distinct from the company's own marketing analytics, though the type of research was sometimes left ambiguous:

> *"We may share such data with our partners or research institutions for purposes that is within our legal basis of legitimate interest."*

Advertising. All apps shared data with third-party advertisers, ranging from anonymous device and interaction data to insights about the user's pregnancy stage. Almost half of the policies (9/19) explicitly stated that personally identifiable information was shared with third-party advertisers, including demographic data, phone numbers, and, in one case, the user's home address. Three pregnancy-tracking apps shared the user's current pregnancy trimester and IP address with third-party ad networks. While ten policies provided explicit assurance that the user's health data would not be shared with advertisers, it was ambiguous as to whether this only applied to health data explicitly entered into the app by the user, or to app usage data from which sensitive insights could be inferred. Typically, app interaction data was not subject to the same level of safeguarding as health data, which could still reveal sensitive information about users if, for instance, they used features relating to miscarriage or abortion.

> *"We may sell or transfer data to advertisers, who will use this data to serve ads relevant to your interests."*

Legal Compliance. Finally, all 19 policies mentioned that apps processed, retained, or shared data to comply with legal requirements and contracts. Specific use-cases included investigating violations of the developer's terms of service, clinical monitoring, or special scenarios where data must be legally shared with a third party to address emergencies and threats. Many policies (13/19) stated that user data might need to be accessed by law enforcement, security authorities, or regulatory agencies in the case of a request or subpoena, but little was explained about the circumstances under which this could happen, or users' rights if it did. In the case of one policy, this contradicted the in-app privacy FAQs, which assured users that their data would never be shared with the government or law enforcement. Only one app explicitly assured users that they would be protected through anonymisation:

> *"We cannot prevent the government from issuing a subpoena, however, we will not be able to produce your period data because we cannot connect it to your login information. We do not know which data set belongs to which person."*

4.2.6 Data Storage and Retention. Apps stored personal data locally on the user's device (7/19), on company servers (15/19), on commercial third-party servers (17/19), and/or at external research facilities (3/19) in various locations, such as the US, EU, and Asia. A total of 15/19 policies addressed the developer's data retention policies. While nine policies provided a specific time frame for data expiration (e.g., 180 days for data relating to interest-based advertisements), the remaining six described broad conditions for determining retention periods relating to legal obligations, the length of service use, and whether the user had requested deletion. Importantly, two policies addressed the impact of app deletion or inactivity on user data, stating that data would be erased after three years. Only four policies provided a description of how data storage and retention varied for registered versus unregistered users, despite several apps providing different back-up options for each type of users (see §4.3.1).

> *"The criteria we use to determine our retention periods include: (i) the length of time you use the Application; (ii) whether there is a legal obligation; or (iii) whether retention is advisable in light of our legal position."*

4.2.7 Data Safeguarding Measures. All but one policy described measures for safeguarding user data against privacy and security threats. Technical safeguarding measures included encryption of data during transit, implementing network security protocols, and de-identification of personal data through means of aggregation, or storing PII separately from app usage data on the developer servers. Organisational security and privacy measures included

adherence to the principle of data minimisation, due diligence and vetting of third parties, as well as adhering to region-specific privacy laws (e.g., GDPR and the CCPA). Despite these assurances, all policies contained liability statements and acknowledgements that the risk of data breaches would be impossible to eliminate. We found that 9/19 policies claimed a lack of responsibility for the practices of any third parties, and shifted the responsibility for reviewing their privacy policies to the user, despite previously claiming to vet third-party vendors and SDKs who accessed user data. Where third-party recipients of user data were named, responsibility for reviewing their policies and terms was typically shifted to the user.

> *"We do not bear responsibility for how third parties use any information that they have obtained from you, and we do not have any control over this."*

4.2.8 User Consent and Opting Out. Consent to the full privacy policy was typically inferred by installation and operation of the app or the creation of an account. Through this, the user consented to sharing their data with third parties; agreeing with third parties' privacy policies; transferring their data outside of their country of residence where different data protection laws might apply; and using data for app promotions. Refusing to accept often meant that the user was unable to access the service altogether.

> *"By creating a profile or registering to use our apps, you expressly agree that we may process the health data you provide [...] this information may be transferred to — and maintained on — computers located outside of Your state, province, or country."*

User consent to the app's privacy policy facilitated automatic consent to the policies of all third parties, despite the high overhead associated with reading and fully understanding these policies. For instance, one app policy listed more than ten different entities that processed user data, and another listed six companies involved in the provision of customer support alone. In both cases, the user was instructed to contact each third-party entity individually if they wished to opt out of their data being processed. Furthermore, some policies described the freedom of third parties to share user data even further with their own advertising networks and beyond. It would be unreasonable to expect that a single checkbox at the time of app installation translated into informed consent to this extensive range of third-party data practices, and yet, 9/19 policies cited user consent as a legal basis for processing data.

We identified different approaches to withdrawing consent to data processing activities. These included directly contacting developers or third parties via email (9/19), tailoring app settings (11/19), and/or using device-level controls (10/19); though these instructions were often vague, not platform-specific, or out-of-date. A common practice for opting out of targeted advertising was changing or disabling the advertising ID on the user's device, causing all ad preferences to be reset device-wide—a potentially undesirable outcome for some users. Some policies phrased instructions in such a way that the user might confuse device settings with their in-app settings, by referring to both in the same sentence, or not clearly distinguishing the two:

> *"You can check the status of your "Allow Access to Device Identifier (IDFA)" permissions in the App under "Me" - "Settings" - "Privacy Settings" and decide to enable or disable the "Allow Access to Device Identifier (IDFA)" permissions at any time."*

Finally, while 11/19 policies stated that users could opt out of non-essential processing such as marketing analytics in the app settings, these mechanisms were either described vaguely or not implemented within the app. As we discuss in the following section (§4.3), only seven apps actually contained granular opt-out settings. Two privacy policies instructed the user to uninstall the app if they wished to opt out of data collection; however, this would not prevent developers from processing historical data as per their retention policies (see §4.2.6).

4.2.9 Data Deletion and Portability. The majority of privacy policies (14/19) addressed users' right to delete their data. However, the language around data deletion was often unclear, with policies using the terms *"deletion"*, *"erasure"*, *"deactivation"*, and *"removal"* interchangeably, and bundling *account* and *data* deletion. Mechanisms for deleting data included contacting the developer via email (9/19), or directly via the app settings (6/19)—though eight apps which implemented deletion buttons made no mention of this feature in the privacy policy. Twelve policies gave details about the developer's compliance process, including how long the data would take to be deleted from the app's servers, and conditions under which the request could not be carried out due to technical or legal reasons. However, this information was often vague. One policy stated that following the termination of an account, the user's personal data would be "deleted **or** anonymised," despite, deletion and anonymisation having different privacy implications should data later be re-accessed.

> *"You can delete your data at any time. To erase your data, simply hit the delete button within your profile. Within minutes your data will be gone permanently.*

Lastly, 12/19 policies mentioned the right to data portability. This involved giving the user a copy of their data in a *"commonly used"*, *"machine readable"*, *"structured"*, or *"portable"* electronic format. However, policies were often ambiguous as to which data could be exported or transferred, or stated that the right only applied to "automated data" without defining what this meant in practice. Only four policies made specific reference to in-app settings or features for exporting data. However, in all cases, these features did not facilitate a full data download, and only allowed subsets (e.g., free-text notes) to be exported (see §4.3.4). In one app, export features were available for Premium iOS users only.

4.3 UI Inspection

In this section, we report on the key findings of our usability inspection. We describe app mechanisms for onboarding and account creation, user privacy controls, and practices for data collection. We also report on the notification management, data deletion, and export mechanisms offered to users.

4.3.1 Onboarding and Account Creation. Out of the 20 apps, 16 included a visible privacy notice and consent mechanism such as a check-box when the app was first opened. However, only five apps provided *granular* consent options for advertising and analytics, with the remaining apps forcing the user to accept or reject the

full privacy policy as a pre-condition for service use (see Fig. 1a). We identified different conventions with respect to registration and authentication across the apps in our sample. Some apps had no option to sign up (7/20), others had optional account creation (10/20), and a few required users to create an account in order to use the service (3/20). One app implemented a special anonymous mode in which only essential tracking data (e.g., cycle dates, symptoms) was backed up on developer servers without any corresponding identifiers such as names or emails. Account creation was described in several UIs as a measure to "*protect*", "*save*", or "*recover*" the user's data in case their device was lost or damaged, since the developers could only externally store the data of registered users (see Fig. 1b). However, in two apps, the optional call for registration was presented as mandatory, and could only be dismissed with a small transparent cross or through tapping the back button.

Often, the registration and onboarding procedure collected more data than was necessary for app function, and failed to clearly indicate when data was optional. For instance, in two apps, users could omit the surname field and sign up with just their first name, but this was not indicated with an optional marker. Thus, the interface was misleading and could cause users to relinquish more data than required. Moreover, one popular period-tracking app onboarded the user with questionnaires that requested highly sensitive data such as how long they had been trying to conceive and whether they had ever lost or terminated a pregnancy. For most questions, there was an option to skip and not disclose—however, it used gray text, which is a typical indication that an option is disabled (see Fig. 1c). Lastly, most apps (13/20) had at least one type of push notification enabled by default, and only three apps proactively encouraged the user to review their notification settings during onboarding. Half of the apps facilitated customisation of the timing, frequency, and message of notifications, allowing the user to configure discreet and manageable push notifications.

4.3.2 Privacy Controls. Only 7/20 apps implemented granular privacy controls that allowed the tailoring of specific privacy preferences (see Fig. 2a). These controls were either proactively presented to users during the initial onboarding process (5/20), or were available in the user's privacy settings (2/20). However, many of these privacy controls had low usability, making it difficult for users to meaningfully engage with their own privacy settings. For instance, controls for opting out of third-party vendors were often presented as lists that were long and complex to read and understand (see Fig. 2b). Non-essential data processing was often enabled by default, with unclear or complex opt-out mechanisms, and privacy control screens were often only accessible through unintuitive interactions. For example, related privacy options could be set in multiple locations within the same app, allowing users to set contradictory preferences—e.g., a user could consent to data sharing with a personalised ad vendor but opt out of personalised advertising on a different screen. Furthermore, in two apps, each consent clause had a single toggle slider labelled *Consent*, which was disabled by default. However, other clauses had an additional slider labelled *Legitimate Interest*—in all cases, this toggle was enabled by default (see Fig. 2c). While the legal definition of a *Legitimate Interest* was made available to the user if they tapped the question mark icon, the explanation did not address the difference between the two provided options.

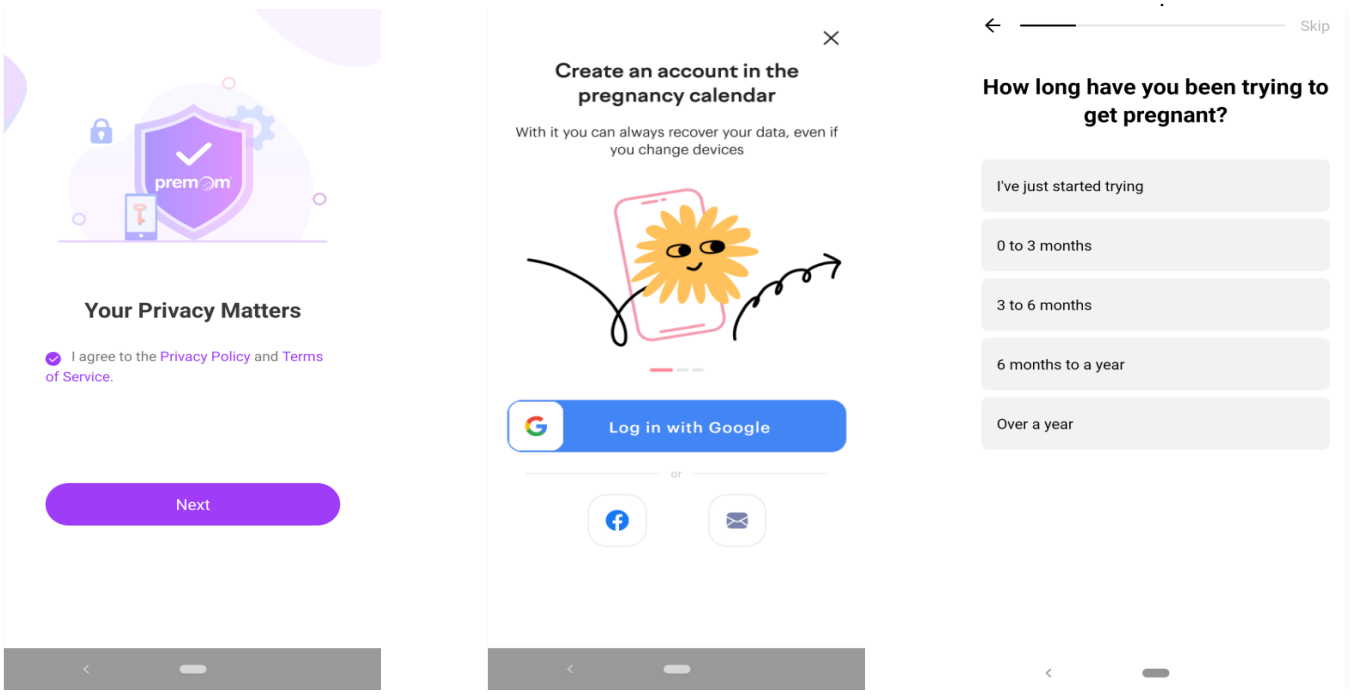
4.3.3 App Data Collection. All apps performed extensive tracking of users' periods, cycles, pregnancies, and other aspects of their lives. This included their sex life, mental health, physiological health, and doctor's appointments, with one app allowing the user to enter the name and speciality of their physician (see Fig. 3a, Fig. 3b, and Fig. 3c). Some fertility-tracking apps allowed the user to track the use of any drugs or intoxicants, and required camera access to photographs of pregnancy and ovulation tests, with no option to record the results manually. Though entering symptom and sex-related data was optional, it was often not clear how it factored into the predictions or charting features of the apps. For instance, six apps provided advanced symptom analysis features but required users to upgrade to premium to access them—one such app allowed intimate sex tracking but provided no visible summary of elements tracked daily.

In addition, we found that 6/20 apps contained community features such as comment threads under articles or in-app forums. If users logged into the app with Google or Facebook, their full names were automatically imported and appeared on forum contributions unless the screen name was changed in their account settings. In several apps with forums, we observed users discussing highly sensitive topics, including past abortions and intimate details about their families. Despite this, only 3/20 apps proactively presented any in-app community guidelines or privacy notices to users before they could start using these forums. We also observed that in 2/20 apps, forum contributions were either available on the web platform, or could be accessed by third-party search engines and APIs. This was not communicated clearly through the interface, meaning that users could assume that their posts would only be visible to other app users.

4.3.4 Data Deletion. We found that 14/20 apps contained an account or data deletion mechanism, typically available in the user's settings or profile screen. However, the option was not always intuitively located: in two apps, the data deletion and export operations were collapsed under a section titled *"Legal"*. Apps typically communicated the effects of deletion operations in terms of permanence and reversibility through a warning pop-up, and the outcome of using the operations was typically consistent with what was communicated. However, in apps with forums, there was no indication of whether users' forum contributions would be deleted, anonymised, or aggregated, and in one app, the user's forum account (which was powered by a third-party provider) was not deleted even when their app account was deleted. By inspecting the deletion practices of the apps in our sample, we identified three overarching techniques for account and data deletion, which differed in terms of data retention and recoverability:

- **Account only.** Four apps only contained a *delete account* function, only available for registered users. This mechanism cleared the app of profile data but could retain some period or pregnancy tracking data, and allowed the user to continue using the app in unregistered mode (see Fig. 4a).
- **Separate options for account and data deletion.** Four apps implemented a *delete data* button available to all users

Figure 1: Examples of app onboarding screens and consent mechanisms.

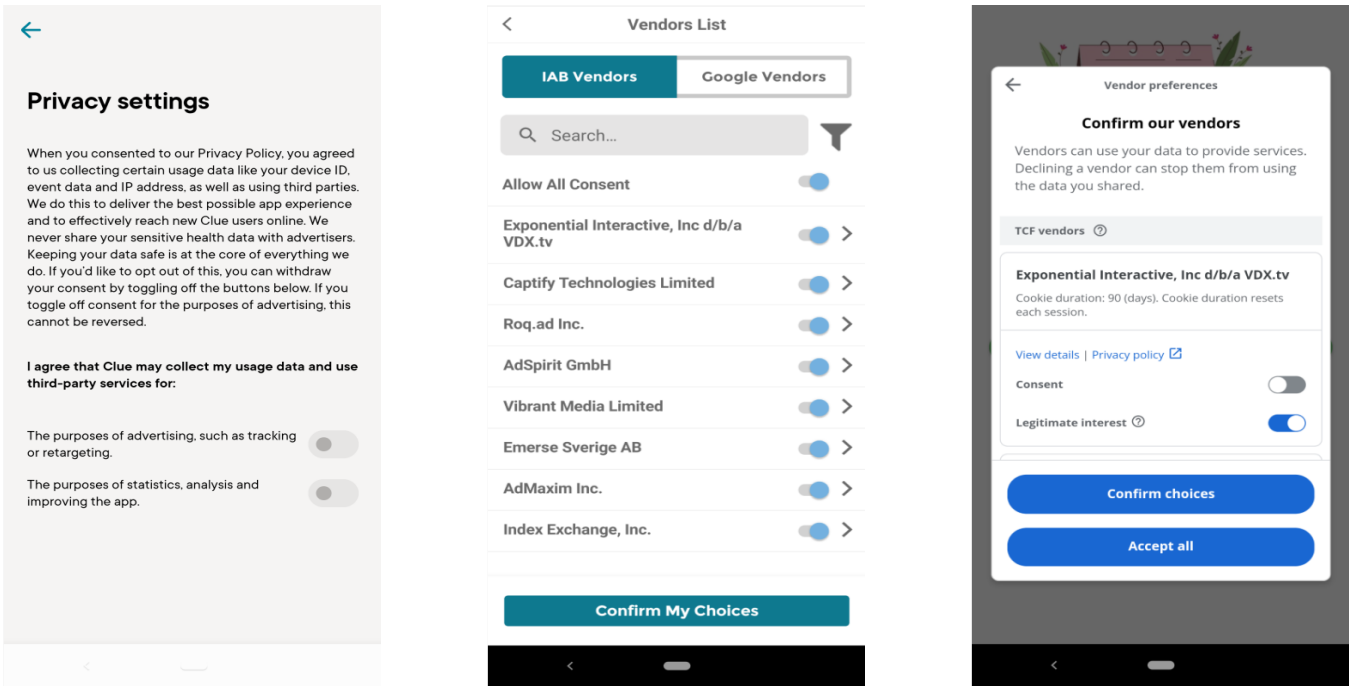


(a) Bundled consent mechanism forcing the user to accept (App #13).

(b) Call to account registration and data back-up (App #11).

(c) Onboarding questionnaire with a grayed-out skip link (App #6).

Figure 2: Examples of app privacy controls and settings.

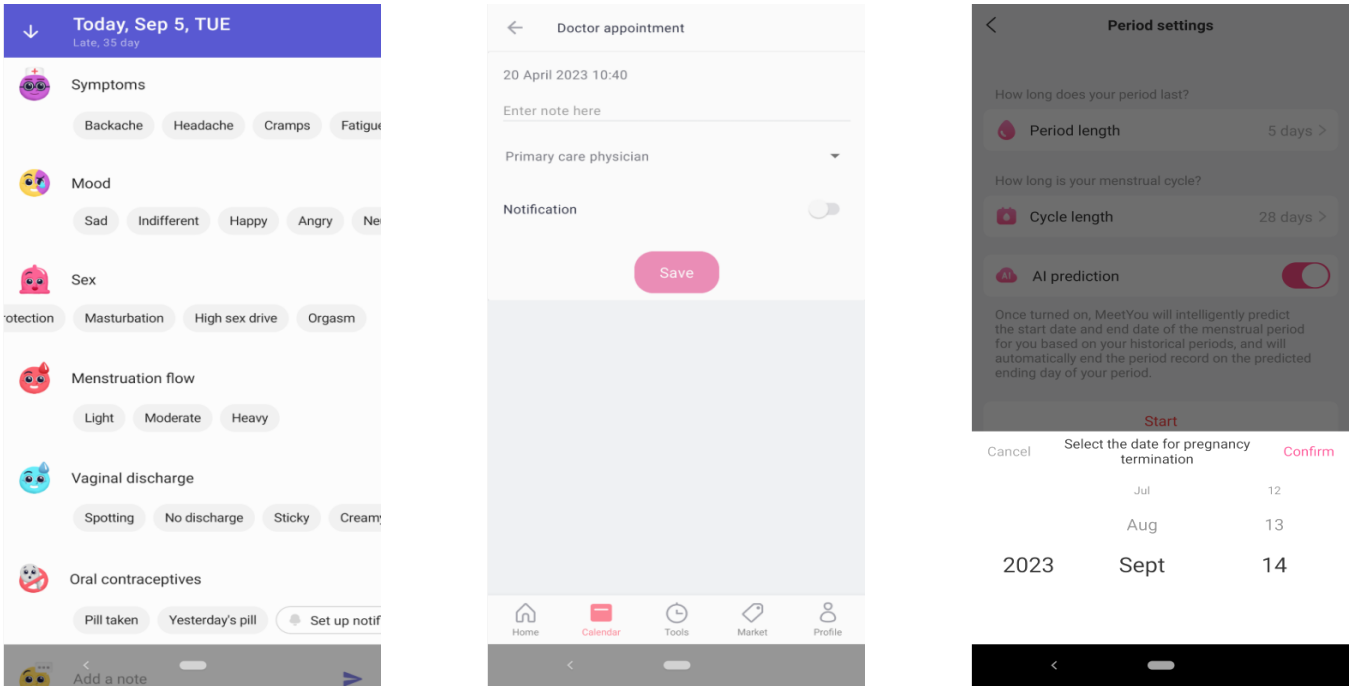


(a) Screen for opting out of targeted advertising and analytics (App #5).

(b) List of third-party vendors with search and filter options (App #4).

(c) Consent mechanism with double toggle sliders (App #1).

Figure 3: Examples of in-app data collection: symptom tracking, physician's details, and pregnancy cancellation.



(a) Example screen for tracking symptoms, menstrual flow, and sexual activity (App #19).

(b) Example screen for entering doctor's appointments and physician name and speciality (App #11).

(c) Pregnancy cancellation screen: the user is required to enter the date of termination to proceed (App #10).

as well as a *delete account* button that was only available to registered users. The *delete data* button removed all data from the device and logged the user out if they were registered. However, when the user re-opened the app, they could log back in with all data re-imported into the device. To delete all data from the device and the cloud, users needed to select an additional *delete account* button (see Fig. 4b).

— **Full deletion.** Six apps contained a single *delete data* option which triggered full and irreversible deletion of account and tracking data (see Fig. 4c).

In addition to account and/or data deletion buttons, pregnancy-tracking apps contained an option which allowed users to stop tracking their pregnancy. The workflow of this option sometimes mirrored that of the data deletion operation. For instance, two apps had identical post-action pop-up messages for the 'data delete' and 'stop pregnancy-tracking' options. We found that 8/20 apps encouraged or required the user to input a reason for stopping their pregnancy tracking, which included the termination or loss of the pregnancy. Concerningly, three apps required users to input the date on which they miscarried or terminated their pregnancy before they could reset the app without providing a reason as to why this declaration was necessary (see Fig. 3c).

4.3.5 Data Portability. Only 8/20 apps provided an in-app mechanism for exporting data into a human or machine-readable format. However, even when data could be exported, it was usually incomplete, and only contained a small selection of the user's health data (e.g., recent menstrual cycle dates). Moreover, three apps made the PDF "health report" feature available for premium users only, and implemented no free mechanism for data portability. Lastly, incompatible data export formats made it challenging to transfer data across different apps. Only two apps provided an option to import data; this feature was often difficult to use due to poor interoperability across apps. For example, one app allowed users to import data as a `.AMC` file, but no other apps allowed data to be exported in this format.

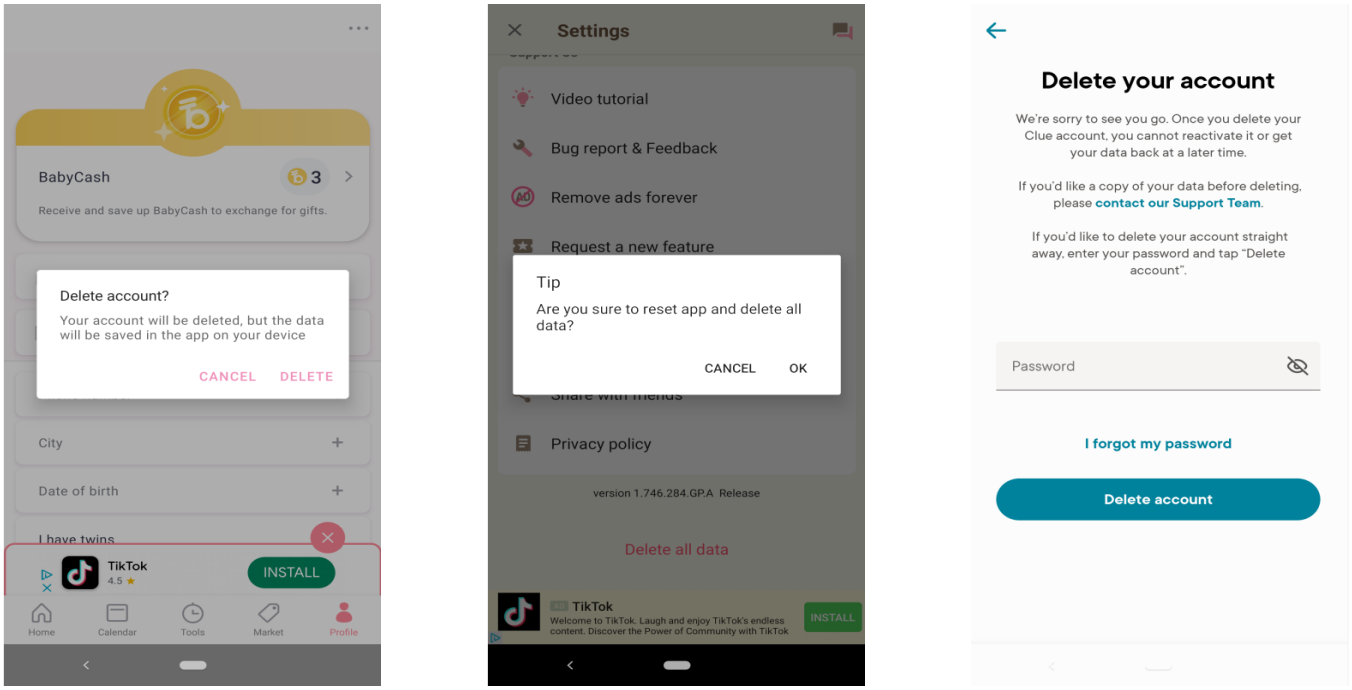
5 DISCUSSION

Our work is the first in the FemTech space to combine a thematic analysis of Data safety sections and privacy policies with a privacy-focused usability inspection of female mHealth apps. Our work constitutes the most detailed analysis to date, and raises design and policy considerations for future work in the FemTech privacy space. We now summarise how our findings compare to and extend previous work, before discussing some of the key implications of our study post-Roe.

5.1 Comparison with Prior Work

Overall, the privacy policies in our sample were not well-tailored to the FemTech genre, and they did not address the unique privacy landscape of this domain. Consistent with past work [2, 29, 85], app privacy policies were often excessively long, and used complex, ambiguous, and technical language which limited comprehension

Figure 4: Examples of data deletion mechanisms with different conventions for data vs. account deletion.



(a) Account only: deleting the user's profile—tracked data remains in the app (App #11).

(b) Separate options: deleting tracked data—user must select another option to delete their account (App #15).

(c) Full deletion: single option triggers full and irreversible account and data deletion (App #4).

of the developers' data practices. Many privacy policies covered multiple apps, websites, or services by the same developer, many of which were unrelated to female health (e.g., games, fitness), framing reproductive health data as a routine piece of data as opposed to data with the potential to stigmatise or criminalise users [85]. Indeed, many of the practices we identified, such as using personal data for cross-platform behavioural analytics and advertising [9], sharing data with law enforcement if necessary [22, 98], non-responses to *Do Not Track (DNT)* signals [101], and issues related to poor readability and historical privacy policy versions being difficult to find [65] are common among privacy policies outside of mHealth apps, and among other systems such as websites and IoT devices. With the exception of few apps that implemented anonymity and privacy-enhancing features, we found limited evidence that female mHealth apps implemented better privacy protections than other types of apps, despite the recent overturning of Roe v. Wade.

In line with prior work in the FemTech space, we found that female mHealth apps collected (and sometimes required) very intimate health data to be entered in combination with uniquely identifying information [2, 3, 30, 85], raising the risk of de-anonymisation and criminalisation [22]. Though prior work has highlighted that period-tracking apps collect behavioural data such as clickpaths and searches [2, 30], we additionally demonstrated that this data could be used to infer pregnancy or intent to have an abortion, and is not yet afforded the same protections as sensitive data entered directly into the app, such as not being shared with third-party advertisers and being subject to deletion and access requests. We also identified a lack of meaningful consent options offered to users, who must accept invasive privacy practices as a pre-condition for using the app—an issue which has persisted over time across the app ecosystem [2, 60, 72].

Amidst the very real risk of user data being turned over to authorities, recent work suggests that users feel more at ease with period-tracking apps that are based in the EU and subject to GDPR [22]. However, this may be a misconception, as our analysis revealed that EU-based apps could still transfer user data to third-party processors based in the US, or to countries where fewer data protection regulations apply. With respect to this work, despite conducting a similar study on female mHealth app privacy post-Roe, Dong et al. [22] focused on a more constrained set of data collection and legal practices, without addressing data safeguarding and privacy rights such as data deletion, data portability, and user consent. Therefore, while our analysis would agree with their finding that privacy policies provide an overwhelmingly comprehensive overview of the types of data *collected* by apps, we identified a wide spectrum of privacy issues, and demonstrated the safety implications of these issues post-Roe. In particular, we identify more disconnects between what is stated in privacy policies and implemented in the app UI with respect to data retention, deletion, portability and opt-out mechanisms. We discuss these issues in the coming sections.

5.2 Disconnects and Inconsistencies Between Privacy Policies and Data Safety Sections

A key finding of our analysis was the presence of inconsistent and conflicting information across privacy policies, Data safety sections, and app interfaces. In particular, we identified disconnects surrounding stated mechanisms for data deletion that were not implemented in the app, and found undisclosed instances of sharing user data with third parties (see §4.1). However, rather than assuming deliberate intent to mislead users, these disconnects could be linked to the conventions of the Data safety section. For example, there exist several exceptions which allow app developers to omit certain data practices when filling out a Data safety form, including practices related to data which is anonymised, shared with the explicit consent of users, or shared for legal purposes [35]. These exemptions might have resulted in key data practices not being disclosed in the Data safety section, such as the sharing of user data with law enforcement. While discrepancies in the Data safety section are not unique to female mHealth apps [92], misleading declarations are particularly consequential around these apps due to the sensitive nature of the data they are processing. Inaccurate or ambiguous information surrounding data practices makes it difficult for users to properly evaluate their risk level.

Previous studies have identified that app developers view the implementation and documentation of privacy practices as a challenging legal requirement [57, 58], and that limited resources and small development teams can contribute to the use of boiler-plate templates for privacy policies [85]. We observed this practice throughout our study, since many developers in our sample appeared to be small businesses which did not specialise in female health. Therefore, we identify a need for future work which explores how female mHealth app developers perceive, document, and implement privacy practices. At a minimum, future work should explore how simplifying the expectations and regulations surrounding Data safety forms may support developers in more accurately reporting their privacy practices on the Google Play Store, to avoid misleading users about activities with safety implications.

5.3 FemTech as a Vehicle for Intimate Surveillance

Consistent with prior work, we found that the data collection practices of female mHealth apps were extensive, capturing users' health, lifestyles and sexual activities [3, 64, 85]. Even when entering intimate data was optional, many apps placed features which meaningfully tracked or analysed these data points behind a paywall. This introduced an asymmetry, in that users disclosed sensitive data that apps could freely re-use for commercial purposes, but were artificially restricted from features allowing them to benefit materially from their own data. However, we observed many cases where users had no choice but to relinquish data. Dark patterns such as not indicating that form fields were optional—were simple yet consequential design manipulations increasing data disclosure. Alarmingly, some pregnancy-tracking apps required users to indicate whether they had miscarried or had an abortion before disabling pregnancy mode, a practice with dire safety implications should a data breach occur.

As per our privacy policy analysis, we identified widespread and covert behavioural tracking, which allowed developers to *create* sensitive information about users as well as collect it directly, through combination and inferential analysis. While prior research shows how tracking for advertising purposes is persistent across mobile app ecosystems [9], the risk these practices present is more pronounced here due to the potential misuse of this data to harm its users. Third parties combining multiple data points invite complexities with regards to data ownership as it becomes increasingly abstracted, aggregated, and interpreted by networks of third parties. Indeed, we found no clear mechanisms for users to discover which inferences an app had made about them, and privacy policies implied that GDPR data access, deletion, and portability requests applied only to data collected directly from users. Therefore, we recommend greater transparency and customisability surrounding the inferences made about users. Users' privacy settings could contain options to remove inferences, control what data is used to create inferences, or opt out of the practice altogether. Sensitive app interactions, defined as those with the potential to uncover high-risk activities in isolation or combined with other data points, should either not be stored or be afforded the same protections as data collected directly from the user.

5.4 Cascading Consent and Changing Privacy Policies

Our analysis revealed several problematic practices surrounding user consent. As we discussed, data collection, processing, and sharing practices of female mHealth apps were extensive, and included the transfer of user data to organisations and third parties which were at liberty to share the data even further as per their privacy policies; a phenomenon to which we refer to as *cascading consent*. As the number of third-party recipients of user data grows, it becomes necessary for the user's consent to "cascade" to more and more unfamiliar data transmission contexts, making it impossible for users to imagine the ecosystems through which their data flows [71]. While not unique to female mHealth apps [77], these practices make it difficult for users to evaluate the risks posed by apps within the context of reproductive rights. Hence, granular and better-designed consent workflows are required in female mHealth apps, as existing mechanisms either offered too few options, or were too complex. As an initial step, we recommend *prioritisation* in privacy controls, with designs placing greater emphasis on data practices which could implicate the user's personal safety (e.g., disclosing reproductive health data to third parties). This could be achieved through implementing a preview of privacy options deemed the most important, with an option to expand and tailor less essential ones.

Furthermore, updates to privacy policies over time can weaken consent if users are not made aware of changes in a timely fashion [72]. Most policies stated that the terms could change unilaterally in the future, and implied that users were responsible for regularly checking for updates; a significant burden, since no policy contained a summary of changes, and past versions of the policy were rarely available. We underscore the importance of proactively informing users of changes to the privacy policy, and providing an accessible and prominent summary of the changes in every version to aid

user's decision-making processes. However, users' dependency on a period-tracking app can be expected to grow over time as they increasingly rely on the technology to track their reproductive health [17, 85], and generate historical data which is necessary for accurate predictions [21]. In such scenarios, users may feel coerced into accepting an updated privacy policy containing concerning privacy practices as an alternative to losing their past data if mechanisms for data portability are poor, as we discuss in the following section.

5.5 Data Retention, Deletion, and Portability Go Hand-in-Hand

The right to be forgotten is vital for users to maintain control over their digital footprint. However, in many apps, this was undermined by design flaws, ambiguous language, and conflating key terms such as 'erase' and 'delete' despite technical and legal differences between these two operations [37]. Data erasure typically refers to removing all copies of data such that it is no longer recoverable, whereas deletion only removes a copy; conflating these two terminologies could contribute to users developing inaccurate mental models of deletion operations [37]. Furthermore, app interfaces and privacy policies lacked transparency around the retention policies which applied to data deletion mechanisms, making it unclear as to whether data would be immediately erased, or kept in a recoverable form for a set time period after users deleted their data and/or account. Notably, two policies stated that data could be kept for an additional *three years* after the app was deleted from a user's device (see §4.2.6)—highlighting flaws in the assumption that deleting a period-tracking app immediately protects users from criminalisation or other related risks [32, 41].

Furthermore, we observed complexities in how data deletion was implemented within apps: six apps offered no in-app mechanism for deletion altogether (with contacting the developer being the only way to request deletion), and others implemented a patchwork of account and data deletion operations with different behaviours and privacy implications (see §4.3.4). While a single mechanism for account deletion that automatically triggers full data deletion is simpler, some users may wish to delete their health data while retaining their accounts or profiles, or may wish to recover their data in the future. This trade-off between simplicity and recoverability must be considered by designers who wish to engineer usable data deletion in their apps.

Lastly, we identified limited options for data portability within the apps in our sample. Options to export data were often hidden behind paywalls, or only supported partial exportation. As discussed in §5.4, data portability is important for app users who require historical data to support period and ovulation predictions, should they wish to discontinue or switch apps due to privacy concerns [32]. As a result, female mHealth apps should provide an in-app mechanism for exporting all data free-of-charge, and better support interoperability across the app ecosystem. Users should also be presented with an option to download a copy of their data before proceeding with account or data deletion (e.g., in a confirmation pop-up), should they wish to resume period tracking in the future.

5.6 Beyond Privacy: User Safety in a Post-Roe World

As discussed extensively in prior work [64, 80, 81], female mHealth apps collect and process highly sensitive data which could implicate not only users, but also their medical providers in contexts where abortion is criminalised. This data not only has privacy implications but also *physical safety risks*, in contrast to other app genres. Discrimination, stigmatisation, blackmail, and physical violence are among some of the worst consequences of mismanaged female mHealth app data (e.g., data breaches or incorrect inferences) that women may face in precarious political and social contexts [3, 19, 22, 64, 81]. Our analysis suggests that the privacy practices of female mHealth apps are not tailored to or commensurate with the unique safety risks posed by these technologies in a post-Roe v. Wade world.

Despite these flaws, we identified some good practices among the apps in our sample, such as explicitly addressing the sensitivity of menstrual data in light of the overturning of Roe v. Wade, and/or making efforts to safeguard users against legal threats. For example, one app (Flo) implemented a dedicated *Anonymous Mode* following the overturning of Roe v. Wade, which provided users with the option to use the app without any identifiable information being stored [40], and another (Stardust) explicitly anonymised any stored health data so it could not be linked to individuals [88]. However, on balance, we found that these measures have not been expanded to the wider female mHealth app ecosystem, which largely frames data as a physical asset to be secured, as opposed to meaningfully safeguarding the individuals from whom data was collected. Similarly, all of the apps that implemented protective measures after the overturning of Roe v. Wade were period- and fertility-tracking apps, despite pregnancy-tracking apps collecting pregnancy termination history and dates, suggesting that this category of app requires greater scrutiny.

Female mHealth apps currently sit at the intersection of health, gender, and policy, and support women who experience barriers to accessing reproductive healthcare [3]. Yet, users find themselves caught in a patchwork of opaque and invasive privacy practices, with app discontinuation the only viable mechanism for meaningfully withdrawing consent. The dependence of many women on these apps, paired with the increasingly risky political climates in which they now live, warrants a greater degree of stewardship over the ***safety*** of users, and innovation around how we may overcome the dominant model of "notice and consent", which currently places a disproportionate privacy burden on users [72, 75]. Future development efforts should include greater involvement of at-risk users through *participatory threat modelling*, to unveil population-specific privacy concerns that may otherwise be overlooked by designers [62, 86]. Keeping with principles of universal design, these shifts could precipitate improvements across wider categories of apps which process sensitive data, including fitness and mental health apps [72].

6 LIMITATIONS & FUTURE WORK

We acknowledge limitations in our study. Firstly, we only included apps available in Google Play in our analysis, to reflect more widespread use of Android devices worldwide. However, there are privacy and security differences across the iOS and Android operating systems [51, 52], making future work which includes popular iOS apps on the Apple App Store valuable. Similarly, while manually analysing privacy policies allowed us to conduct a more grounded and in-depth investigation into app privacy practices, future work could upscale our approach, using our codebook to automate the analysis of a larger set of privacy policies, and conduct quantitative linguistic analysis to produce metrics for policy readability and complexity [85]. This could also support longitudinal analysis that tracks changes in privacy policies over time, and comparisons across different categories of female mHealth apps, as our analysis revealed invasive practices in pregnancy apps, such as requesting the date of a termination.

Furthermore, our usability inspection was conducted by the research team and did not involve the direct input of users. Therefore, our analysis did not perfectly mirror typical daily usage, which may have uncovered design flaws that could emerge from regular long-term app use. In future work, we plan to conduct a user study, to understand the privacy perceptions and mental models of female mHealth app users. We also plan to conduct a follow-up interview study with female mHealth app developers to understand the impact of the overturning of Roe v. Wade on operational practices, as well as challenges associated with navigating privacy legislation when considering the sensitive nature of female health data [93]. We will also further investigate whether developers write their own app privacy policies and, if not, to whom they delegate this task [4], given the inconsistencies we identified between the information declared in the Data safety sections (see Table 1) and privacy policies. Lastly, legal specialists were not formally involved in the research. Given many legal nuances in our findings, future work should consult legal specialists to consider how different geographic locations of app developers or servers and their corresponding jurisdictions could implicate users.

7 CONCLUSION

In this work, we explored the privacy practices of female mHealth apps, with an emphasis on how intimate user data is collected, shared, stored, and safeguarded by developers and third-parties in a post-Roe world, and the data rights offered to users. Through an in-depth, comparative analysis of the Data safety sections, privacy policies, and interfaces of 20 popular apps, we uncovered several inconsistencies, as well as problematic privacy practices which saw data transmitted through complex chains of third-parties. We also identified substantial shortcomings in the design of female mHealth app interfaces, including a lack of granular consent, inconsistent mechanisms for data deletion and portability, and dark patterns which coerced users into entering sensitive data. Our work demonstrates how intersections of gender, technology, and policy can configure unique risks to female mHealth app users in a post-Roe world, and we provide recommendations and avenues for future inquiry that promote a humanistic and safety-conscious approach to developing health technologies.

ACKNOWLEDGMENTS

This research was supported in part by an unrestricted gift from Google.

REFERENCES

[1] Ruba Abu-Salma, Kat Krol, Simon Parkin, Victoria Koh, Kevin Kwan, Jazib Mahboob, Zahra Traboulsi, and M. Angela Sasse. 2017. The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram. In *Proceedings 2nd European Workshop on Usable Security (EuroUSEC'17)* (April 29, 2017, Paris, France). Internet Society. https://doi.org/10.14722/eurousec.2017.23006

[2] Najd Alfawzan, Markus Christen, Giovanni Spitale, and Nikola Biller-Andorno. 2022. Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis. *JMIR mHealth and uHealth* 10, 5 (May 2022), e33735. https://doi.org/10.2196/33735

[3] Teresa Almeida, Laura Shipp, Maryam Mehrnezhad, and Ehsan Toreini. 2022. Bodies Like Yours: Enquiring Data Privacy in FemTech. In *Adjunct Proceedings of the 2022 Nordic Human-Computer Interaction Conference (NordiCHI '22)* (October 8 - 12, 2022, Aarhus, Denmark). ACM, New York, NY, USA, 1–5. https://doi.org/10.1145/3547522.3547674

[4] Noura Alomar and Serge Egelman. 2022. Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps. *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2022, 4 (2022), 250–273. https://petsymposium.org/popets/2022/popets-2022-0108.php

[5] Apple. 2023. *Privacy Labels - Apple.* https://www.apple.com/uk/privacy/labels/

[6] Oshrat Ayalon, Sophie Li, Bart Preneel, and Elissa M. Redmiles. 2023. Not Only for Contact Tracing: Use of Belgium's Contact Tracing App among Young Adults. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 6, 4, Article 202 (Jan. 2023), 26 pages. https://doi.org/10.1145/3570348

[7] Oshrat Ayalon, Dana Turjeman, and Elissa M. Redmiles. 2023. Exploring Privacy and Incentives Considerations in Adoption of COVID-19 Contact Tracing Apps. In *32nd USENIX Security Symposium (USENIX Security 23)* (August 9–11, 2023, Anaheim, CA, USA). USENIX Association, USA, 517–534. https://www.usenix.org/conference/usenixsecurity23/presentation/ayalon

[8] Susanne Barth, Dan Ionita, and Pieter Hartel. 2022. Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines. *ACM Comput. Surv.* 55, 3, Article 63 (Feb. 2022), 37 pages. https://doi.org/10.1145/3502288

[9] Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, and Nigel Shadbolt. 2018. Third Party Tracking in the Mobile Ecosystem. In *Proceedings of the 10th ACM Conference on Web Science (WebSci '18')* (May 27–30, 2018, Amsterdan, Netherlands,). ACM, New York, NY, USA, 23–31. https://doi.org/10.1145/3201064.3201089

[10] Claudia Bischoff, Eva Gerlitz, and Matthew Smith. 2020. Vision: I Don't Want to Use My Phone! A Cognitive Walkthrough for YubiKeys. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (September 7 - 11, 2020, Genoa, Italy). IEEE, New York, NY, USA, 160–165. https://doi.org/10.1109/EuroSPW51379.2020.00029

[11] Marilyn Hughes Blackmon, Peter G. Polson, Muneo Kitajima, and Clayton Lewis. 2002. Cognitive Walkthrough for the Web. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'02)* (April 20 - 25, 2002, Minneapolis, Minnesota, USA). ACM, New York, NY, USA, 463–470. https://doi.org/10.1145/503376.503459

[12] Jasmine Bowers, Bradley Reaves, Imani N. Sherman, Patrick Traynor, and Kevin Butler. 2017. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Services. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).* (July 12–14, 2017, Santa Clara, CA). USENIX Association, USA, 97–114. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bowers

[13] British Pregnancy Advisory Service (BPAS). 2012. *Britain's Abortion Law.* https://www.bpas.org/get-involved/campaigns/briefings/abortion-law/

[14] Elizabeth Brown. 2021. The Femtech Paradox: How Workplace Monitoring Threatens Women's Equity. *Jurimetrics* 61, 3 (2021), 289–329. https://heinonline.org/HOL/LandingPage?handle=hein.journals/juraba61&div=18&id=&page=

[15] Ann Cavoukian. 2012. Privacy by Design [Leading Edge]. *IEEE Technology and Society Magazine* 31, 4 (Dec. 2012), 18–19. https://doi.org/10.1109/mts.2012.2225459

[16] Google Help Center. [n. d.]. *Provide Information for Google Play's Data safety section.* https://support.google.com/googleplay/android-developer/answer/10787469?hl=en

[17] Mayara Costa Figueiredo, Thu Huynh, Anna Takei, Daniel A Epstein, and Yunan Chen. 2021. Goals, Life Events, and Transitions: Examining Fertility Apps for Holistic Health Tracking. *JAMIA Open* 4, 1 (Mar. 2021), ooab013. https://doi.org/10.1093/jamiaopen/ooab013

[18] David Cox. 2022. How Overturning Roe *v* Wade has Eroded Privacy of Personal Data. *BMJ* (Aug. 2022), 378:o2075. https://doi.org/10.1136/bmj.o2075

[19] Mary Crossley. 2005. Discrimination Against the Unhealthy in Health Insurance. *Kansas Law Review* 54 (Jul. 2005), 73. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1167043

[20] No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data. 2020. *Privacy International*. https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data

[21] Anne A. H. de Hond, Artuur M. Leeuwenberg, Lotty Hooft, Ilse M. J. Kant, Steven W. J. Nijman, Hendrikus J. A. van Os, Jiska J. Aardoom, Thomas P. A. Debray, Ewoud Schuit, Maarten van Smeden, Johannes B. Reitsma, Ewout W. Steyerberg, Niels H. Chavannes, and Karel G. M. Moons. 2022. Guidelines and Quality Criteria for Artificial Intelligence-based Prediction Models in Healthcare: A Scoping Review. *NPJ Digital Medicine* 5, 1 (Jan. 2022), 2. https://doi.org/10.1038/s41746-021-00549-7

[22] Zikan Dong, Liu Wang, Hao Xie, Guoai Xu, and Haoyu Wang. 2022. Privacy Analysis of Period Tracking Mobile Apps in the Post-Roe v. Wade Era. In *37th IEEE/ACM International Conference on Automated Software Engineering (ASE '22)* (October 10 - 14, 2022, Rochester, MI, USA). ACM, New York, NY, USA, 1–6. https://doi.org/10.1145/3551349.3561343

[23] Samuel Dooley, Dana Turjeman, John P Dickerson, and Elissa M. Redmiles. 2022. Field Evidence of the Effects of Privacy, Data Transparency, and Pro-Social Appeals on COVID-19 App Attractiveness. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI'22)* (April 29 - May 5 2022, New Orleans, LA, USA). ACM, New York, NY, USA, Article 622, 21 pages. https://doi.org/10.1145/3491102.3501869

[24] Sarah Earle, Hannah R Marston, Robin Hadley, and Duncan Banks. 2021. Use of Menstruation and Fertility App Trackers: A Scoping Review of the Evidence. *BMJ Sexual & Reproductive Health* 47, 2 (Apr. 2021), 90–101. https://doi.org/10.1136/bmjsrh-2019-200488

[25] Fahimeh Ebrahimi and Anas Mahmoud. 2022. Unsupervised Summarization of Privacy Concerns in Mobile Application Reviews. In *37th IEEE/ACM International Conference on Automated Software Engineering (ASE '22)* (October 10 - 14, 2022, Rochester, MI, USA). ACM, New York, NY, USA, 1–12. https://doi.org/10.1145/3551349.3561155

[26] Daniel A. Epstein, Nicole B. Lee, Jennifer H. Kang, Elena Agapie, Jessica Schroeder, Laura R. Pina, James Fogarty, Julie A. Kientz, and Sean Munson. 2017. Examining Menstrual Tracking to Inform the Design of Personal Informatics Tools. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)* (May 6 - 11, 2017, Denver, Colorado, USA). ACM, New York, NY, USA, 6876–6888. https://doi.org/10.1145/3025453.3025635

[27] Jacob Erickson, Jewel Y. Yuzon, and Tamara Bonaci. 2022. What You Do Not Expect When You Are Expecting: Privacy Analysis of Femtech. *IEEE Transactions on Technology and Society* 3, 2 (Jun. 2022), 121–131. https://doi.org/10.1109/tts.2022.3160928

[28] Carlos Bermejo Fernandez, Tristan Braud, and Pan Hui. 2022. Implementing GDPR for Mobile and Ubiquitous Computing. In *Proceedings of the 23rd Annual International Workshop on Mobile Computing Systems and Applications (HotMobile '22)* (March 9 - 10, 2022, Tempe, Arizona). ACM, New York, NY, USA, 88–94. https://doi.org/10.1145/3508396.3512880

[29] Leah R. Fowler, Charlotte Gillard, and Stephanie R. Morain. 2020. Readability and Accessibility of Terms of Service and Privacy Policies for Menstruation-Tracking Smartphone Applications. *Health Promotion Practice* 21, 5 (Sept. 2020), 679–683. https://doi.org/10.1177/1524839919899924

[30] Sarah Fox, Noura Howell, Richmond Wong, and Franchesca Spektor. 2019. Vivewell: Speculating Near-Future Menstrual Tracking through Current Data Practices. In *Proceedings of the 2019 on Designing Interactive Systems Conference (DIS '19)* (June 23 - 28, 2019, San Diego, CA, USA). ACM, New York, NY, USA, 541–552. https://doi.org/10.1145/3322276.3323695

[31] Christian Fuchs and Marianna Obrist. 2010. HCI and Society: Towards a Typology of Universal Design Principles. *International Journal of Human–Computer Interaction* 26, 6 (May 2010), 638–656. https://doi.org/10.1080/10447311003781334 arXiv:https://doi.org/10.1080/10447311003781334

[32] Flora Garamvolgyi. 2022. *Why US Women are Deleting their Period Tracking Apps*. https://www.theguardian.com/world/2022/jun/28/why-us-woman-are-deleting-their-period-tracking-apps

[33] Gdpr.eu. [n. d.]. *General Data Protection Regulation (GDPR)*. https://gdpr.eu/tag/gdpr/

[34] Julia Gomula, Mark Warner, and Ann Blandford. 2024. Women's Use of Online Health and Social Media Resources to Make Sense of Their Polycystic Ovary Syndrome (PCOS) Diagnosis: A Qualitative Study. *BMC Women's Health* (2024), 1–13.

[35] Google. [n. d.]. *Provide information for Google Play's Data safety section*. https://support.google.com/googleplay/android-developer/answer/10787469?hl=en-GB#zippy=%2Cdata-types%2Cpurposes%2Cdata-collection%2Cdata-sharing

[36] Gov.uk. [n. d.]. *Data Protection: The Data Protection Act*. https://www.gov.uk/data-protection

[37] Andreas Gutmann and Mark Warner. 2019. Fight to be Forgotten: Exploring the Efficacy of Data Erasure in Popular Operating Systems. In *7th Annual Privacy Forum (APF '19)* (June 13–14, 2019, Rome, Italy). Springer, New York, NY, USA, 45–58.

[38] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a Scavenger Hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)* (April 25 - 30, 2020, Honolulu, HI, USA). ACM, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376511

[39] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An Empirical Analysis of Data Deletion and Opt-out Choices on 150 Websites. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS'19)* (August 12 - 13, 2019, Santa Clara, CA, USA). USENIX Association, USA, 387–406.

[40] Flo Health. [n. d.]. *Anonymous Mode FAQ*. https://flo.health/privacy-portal/anonymous-mode-faq

[41] Kashmir Hill. 2023. *Deleting Your Period Tracker Won't Protect You*. https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html

[42] Kevin K.W. Ho, Dickson K. W. Chiu, and Kristina C. L. Sayama. 2023. When Privacy, Distrust, and Misinformation Cause Worry About Using COVID-19 Contact-Tracing Apps. *IEEE Internet Computing* (Jan. 2023), 1–7. https://doi.org/10.1109/mic.2022.3225568

[43] Tasha Hollingsed and David G. Novick. 2007. Usability Inspection Methods after 15 Years of Research and Practice. In *Proceedings of the 25th Annual ACM International Conference on Design of Communication (SIGDOC'07)* (October 22 - 24, 2007, El Paso, Texas, USA). ACM, New York, NY, USA, 249–255. https://doi.org/10.1145/1297144.1297200

[44] Yue Huang, Borke Obada-Obieh, Elissa M. Redmiles, Satya Lokam, and Konstantin Beznosov. 2022. COVID-19 Information-Tracking Solutions: A Qualitative Investigation of the Factors Influencing People's Adoption Intention. In *Proceedings of the 2022 Conference on Human Information Interaction and Retrieval (CHIIR '22)* (March 14 - 18, 2022, Regensburg, Germany). ACM, New York, NY, USA, 12–24. https://doi.org/10.1145/3498366.3505756

[45] Duha Ibdah, Nada Lachtar, Satya Meenakshi Raparthi, and Anys Bacha. 2021. "Why Should I Read the Privacy Policy, I Just Need the Service": A Study on Attitudes and Perceptions Toward Privacy Policies. *IEEE Access* 9 (Nov. 2021), 166465–166487. https://doi.org/10.1109/access.2021.3130086

[46] Information Commissioner's Office (ICO). 2023. *ICO to Review Period and Fertility Tracking Apps as Poll Shows more than Half of Women are Concerned over Data Security*. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/09/ico-to-review-period-and-fertility-tracking-apps/

[47] Gabriel Kaptchuk, Daniel G. Goldstein, Eszter Hargittai, Jake M. Hofman, and Elissa M. Redmiles. 2022. How Good is Good Enough? Quantifying the Impact of Benefits, Accuracy, and Privacy on Willingness to Adopt COVID-19 Decision Aids. *Digital Threats* 3, 3, Article 27 (Mar. 2022), 18 pages. https://doi.org/10.1145/3488307

[48] Claire-Marie Karat, Robert Campbell, and Tarra Fiegel. 1992. Comparison of Empirical Testing and Walkthrough Methods in User Interface Evaluation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'92)* (May 3 - 7, 1992, Monterey, California, USA). ACM, New York, NY, USA, 397–404. https://doi.org/10.1145/142750.142873

[49] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS'09)* (July 15 - 17, 2009, Mountain View, California, USA). ACM, New York, NY, USA, Article 4, 12 pages. https://doi.org/10.1145/1572532.1572538

[50] Konrad Kollnig, Reuben Binns, Max Van Kleek, Ulrik Lyngs, Jun Zhao, Claudine Tinsman, and Nigel Shadbolt. 2021. Before and After GDPR: Tracking in Mobile Apps. *Internet Policy Review* 10, 4 (2021), arXiv:2112.11117. https://doi.org/10.48550/arxiv.2112.11117

[51] Konrad Kollnig, Anastasia Shuba, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. 2021. Are iPhones Really Better for Privacy? Comparative Study of iOS and Android Apps. *In Proceedings on Privacy Enhancing Technologies (PoPETs)* (2021), arXiv:2109.13722. https://doi.org/10.48550/arxiv.2109.13722

[52] Sophia Kununka, Nikolay Mehandjiev, and Pedro Sampaio. 2018. *A Comparative Study of Android and iOS Mobile Applications' Data Handling Practices Versus Compliance to Privacy Policy*. Springer International Publishing, Cham, 301–313. https://doi.org/10.1007/978-3-319-92925-5_20

[53] Bloomberg Law. [n. d.]. *California Consumer Privacy Laws*. https://pro.bloomberglaw.com/brief/california-consumer-privacy-laws-ccpa-cpra/

[54] Natasa Lazarevic, Marie Lecoq, Céline Bœhm, and Corinne Caillaud. 2023. Pregnancy Apps for Self-Monitoring: Scoping Review of the Most Popular Global Apps Available in Australia. *International Journal of Environmental Research and Public Health* 20, 2 (Jan. 2023), 1012. https://doi.org/10.3390/ijerph20021012

[55] Johanna Levy and Nuria Romo-Avilés. 2019. A Good Little Tool to Get to Know Yourself a Bit Better": a Qualitative Study on Users' Experiences of App-supported Menstrual Tracking in Europe. *BMC Public Health* 19, 1 (Dec. 2019), 1213. https://doi.org/10.1186/s12889-019-7549-8

[56] Karen Levy. 2015. Intimate Surveillance. *Idaho Law Review* 51, 3 (Sep. 2015). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2834354

[57] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I. Hong. 2021. How Developers Talk About Personal Data and What It Means for User Privacy: A Case Study of a Developer Forum on Reddit. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW, Article 220, 28 pages. https://doi.org/10.1145/3432919

[58] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong. 2022. Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI'22)* (April 29 - May 5, 2022, New Orleans, LA, USA). ACM, New York, NY, USA, Article 588, 24 pages. https://doi.org/10.1145/3491102.3502012

[59] Georgianna E Lin, Elizabeth D Mynatt, and Neha Kumar. 2022. Investigating Culturally Responsive Design for Menstrual Tracking and Sharing Practices Among Individuals with Minimal Sexual Education. In *CHI Conference on Human Factors in Computing Systems* (April 29 - May 5, 2022, New Orleans, LA, USA). ACM, New York, NY, USA, 1–15. https://doi.org/10.1145/3491102.3501824

[60] Yue Liu. 2014. User Control of Personal Information Concerning Mobile-App: Notice and Consent? *Computer Law & Security Review* 30, 5 (Oct. 2014), 521–529. https://doi.org/10.1016/j.clsr.2014.07.008

[61] Aleecia M. McDonald and Lorrie Faith Cranor. 2009. The Cost of Reading Privacy Policies. https://api.semanticscholar.org/CorpusID:197633124

[62] Nora Mcdonald and Nazanin Andalibi. 2023. "I Did Watch 'The Handmaid's Tale'": Threat Modeling Privacy Post-Roe in the United States. *ACM Transactions on Computer-Human Interaction* 30, 4, Article 63 (Mar. 2023). https://doi.org/10.1145/3589960

[63] Terry McGovern. 2022. Overturning Roe *v* Wade Has Had an Immediate Chilling Effect on Reproductive Healthcare. *BMJ* (Jun. 2022), 377:o1622. https://doi.org/10.1136/bmj.o1622

[64] Maryam Mehrnezhad and Teresa Almeida. 2021. Caring for Intimate Data in Fertility Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (May 8 - 13, 2021, Yokohama, Japan). ACM, New York, NY, USA, 1–11. https://doi.org/10.1145/3411764.3445132

[65] Abraham Mhaidli, Selin Fidan, An Doan, Gina Herakovic, Mukund Srinath, Lee Matheson, Shomir Wilson, and Florian Schaub. 2023. Researchers' Experiences in Analyzing Privacy Policies: Challenges and Opportunities. *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2023, 4 (Oct. 2023), 287–305. https://doi.org/10.56553/popets-2023-0111

[66] Jaron Mink, Amanda Rose Yuile, Uma Pal, Adam J Aviv, and Adam Bates. 2022. Users Can Deduce Sensitive Locations Protected by Privacy Zones on Fitness Tracking Apps. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)* (April 29 - May 5, 2022, New Orleans, LA, USA). ACM, New York, NY, USA, 1–21. https://doi.org/10.1145/3491102.3502136

[67] Miro. [n. d.]. *Miro*. https://miro.com/

[68] Diana P. Moniz, Maryam Mehrnezhad, and Teresa Almeida. 2023. Intimate Data: Exploring Perceptions of Privacy and Privacy-Seeking Behaviors Through the Story Completion Method. In *Human-Computer Interaction – INTERACT 2023* (August 28 – September 1, 2023, York, UK). Springer Nature, Cham, Switzerland, 533–543.

[69] Mozilla. 2022. *Talkspace Privacy and Security*. https://foundation.mozilla.org/en/privacynotincluded/talkspace/

[70] Jakob Nielsen and Rolf Molich. 1990. Heuristic Evaluation of User Interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '90)* (April 1 - 5, 1990, Seattle, Washington, USA). ACM, New York, NY, USA, 249–256. https://doi.org/10.1145/97243.97281

[71] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79, 1 (2004).

[72] Leysan Nurgalieva, David O'Callaghan, and Gavin Doherty. 2020. Security and Privacy of mHealth Applications: A Scoping Review. *IEEE Access* 8 (Jun. 2020), 104247–104268. https://doi.org/10.1109/access.2020.2999934

[73] Jonathan A. Obar and Anne Oeldorf-Hirsch. 2020. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication and Society* 23, 1 (Jun. 2020), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

[74] State of California Department of Justice. [n. d.]. *California Consumer Privacy Act (CCPA)*. https://oag.ca.gov/privacy/ccpa

[75] Ehimare Okoyomon, Nikita Samarin, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, Irwin Reyes, Álvaro Feal, and Serge Egelman. 2019. On The Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies. In *The Workshop on Technology and Consumer Protection (ConPro '19), in conjunction with the 39th IEEE Symposium on Security and Privacy.* (May 23, 2019, San Francisco, CA, USA). https://api.semanticscholar.org/CorpusID:150370978

[76] Lisa Parker, Vanessa Halter, Tanya Karliychuk, and Quinn Grundy. 2019. How Private is Your Mental Health App Data? An Empirical Study of Mental Health App Privacy Policies and Practices. *International Journal of Law and Psychiatry* 64 (May 2019), 198–204. https://doi.org/10.1016/j.ijlp.2019.04.002

[77] Jennifer Pybus and Mark Coté. 2022. Did You Give Permission? Datafication in the Mobile Ecosystem. *Information, Communication & Society* 25, 11 (2022), 1650–1668.

[78] Kopo Marvin Ramokapane, Awais Rashid, and Jose Miguel Such. 2017. "I feel stupid I can't delete...": A Study of Users' Cloud Deletion Practices and Coping Strategies. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* (July 12–14, 2017, Santa Clara, CA, USA). USENIX Association, USA, 241–256. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/ramokapane

[79] Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James Graves, Fei Liu, Aleecia McDonald, Thomas Norton, Rohan Ramanath, N. Cameron Russell, Norman Sadeh, and Florian Schaub. 2014. Disagreeable Privacy Policies: Mismatches between Meaning and Userss Understanding. *Berkeley Technology Law Journal* 30 (Mar. 2014). https://doi.org/10.2139/ssrn.2418297

[80] Celia Rosas. 2019. *The Future is Femtech: Privacy and Data Security Issues Surrounding Femtech Applications*. Technical Report. https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1193&context=hastings_business_law_journal

[81] Allysan Scatterday. 2022. This is No Ovary-Action: Femtech Apps Need Stronger Regulations to Protect Data and Advance Public Health Goals. *North Carolina Journal of Law & Technology* 23, 3 (2022), 636. https://scholarship.law.unc.edu/ncjolt/vol23/iss3/6

[82] Brennan Schaffner, Neha A. Lingareddy, and Marshini Chetty. 2022. Understanding Account Deletion and Relevant Dark Patterns on Social Media. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (Nov. 2022), 1–43. https://doi.org/10.1145/3555142

[83] Sam Schechner and Mark Secada. 2019. You Give Apps Sensitive Personal Information. Then They Tell Facebook. *The Wall Street Journal* (Feb. 2019). https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636

[84] Andrew Sears. 1997. Heuristic Walkthroughs: Finding the Problems Without the Noise. *International Journal of Human-Computer Interaction* 9, 3 (Sept. 1997), 213–234. https://doi.org/10.1207/s15327590ijhc0903_2

[85] Laura Shipp and Jorge Blasco. 2020. How Private is your Period?: A Systematic Analysis of Menstrual App Privacy Policies. *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2020, 4 (Oct. 2020), 491–510. https://doi.org/10.2478/popets-2020-0083

[86] Julia Slupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. 2022. "They Look at Vulnerability and Use That to Abuse You'': Participatory Threat Modelling with Migrant Domestic Workers. In *31st USENIX Security Symposium (USENIX Security 22)* (August 10–12, 2022, Boston, MA, USA). USENIX Association, USA, 323–340. https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-vulnerability

[87] Mukund Srinath, Lee Matheson, Pranav Narayanan Venkit, Gabriela Zanfir-Fortuna, Florian Schaub, C. Lee Giles, and Shomir Wilson. 2023. Privacy Now or Never: Large-Scale Extraction and Analysis of Dates in Privacy Policy Text. In *Proceedings of the ACM Symposium on Document Engineering 2023 (DocEng '23)* (August 22 - 25, 2023, Limerick, Ireland). ACM, New York, NY, USA, Article 24, 4 pages. https://doi.org/10.1145/3573128.3609342

[88] Stardust. [n. d.]. *Privacy Policy*. https://stardust.app/privacy-policy.html

[89] Statista. [n. d.]. *Software developer gender distribution worldwide as of 2022*. https://www.statista.com/statistics/1126823/worldwide-developer-gender/

[90] Statista. 2023. *Global Market Share Held by Mobile Operating Systems from 1st Quarter 2009 to 2nd Quarter 2023*. https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

[91] Borce Stojkovski, Ruba Abu-Salma, Karen Triquet, and Gabriele Lenzini. 2022. "Unless One Does the Research, It May Seem as Just a Useless Battery-consuming App"–Field Notes on COVID-19 Contact Tracing Applications. *Digital Threats: Research and Practice (DTRAP)* 3, 3 (Sep. 2022), 1–17.

[92] Anne Stopper and Jen Caltrider. [n. d.]. *See No Evil: Loopholes in Google's Data Safety Labels Keep Companies in the Clear and Consumers in the Dark*. https://foundation.mozilla.org/en/campaigns/googles-data-safety-labels/

[93] Mohammed Tahaei, Ruba Abu-Salma, and Awais Rashid. 2023. Stuck in the Permissions With You: Developer & End-User Perspectives on App Permissions & Their Privacy Ramifications. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)* (April 23–28, 2023, Hamburg, Germany). ACM, New York, NY, USA, 24 pages. https://arxiv.org/abs/2301.06534

[94] Tobi Thomas. 2023. *Outrage at Jail Sentence for Woman Who Took Abortion Pills Later than UK Limit*. https://www.theguardian.com/world/2023/jun/12/woman-in-uk-jailed-for-28-months-over-taking-abortion-pills-after-legal-time-limit

[95] Anupriya Tuli, Surbhi Singh, Rikita Narula, Neha Kumar, and Pushpendra Singh. 2022. Rethinking Menstrual Trackers Towards Period-Positive Ecologies. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*

(CHI '22) (April 29 - May 5 2022, New Orleans, LA, USA). ACM, New York, NY, USA, 1–20. https://doi.org/10.1145/3491102.3517662

[96] Lev Velykoivanenko, Kavous Salehzadeh Niksirat, Noé Zufferey, Mathias Humbert, Kévin Huguenin, and Mauro Cherubini. 2021. Are Those Steps Worth Your Privacy?: Fitness-Tracker Users' Perceptions of Privacy and Utility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 4 (Dec. 2021), 1–41. https://doi.org/10.1145/3494960

[97] Maximiliane Windl, Niels Henze, Albrecht Schmidt, and Sebastian S. Feger. 2022. Automating Contextual Privacy Policies: Design and Evaluation of a Production Tool for Digital Consumer Privacy Awareness. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)* (April 29 - May 5 2022, New Orleans, LA, USA). ACM, New York, NY, USA, 1–18. https://doi.org/10.1145/3491102.3517688

[98] Stephanie Winkler and Sherali Zeadally. 2016. Privacy Policy Analysis of Popular Web Platforms. *IEEE Technology and Society Magazine* 35, 2 (Jun. 2016), 75–85. https://doi.org/10.1109/mts.2016.2554419

[99] Pieter Wolters. 2018. The Control by and Rights of the Data Subject Under the GDPR. *Journal of Internet Law* 22, 1 (2018), 7–18.

[100] Richmond Y. Wong, Andrew Chong, and R. Cooper Aspegren. 2023. Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW (Apr. 2023), 1–26. https://doi.org/10.1145/3579515

[101] Your Privacy Policy Must Include a D̈o Not Track(D̈NT) Clause. 2022. . https://www.privacypolicies.com/blog/privacy-policy-dnt-do-not-track/ Last Accessed 12/06/2023.

[102] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman Sadeh. 2022. How Usable Are iOS App Privacy Labels? *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2022, 4 (Oct. 2022), 204–228. https://doi.org/10.56553/popets-2022-0106

APPENDIX A: APP METADATA

Table A.1: Details of female mHealth apps selected for analysis including their genres, developers, and popularity statistics.

ID	App Name	Genre	Dev. Name	Dev. Type	Released	Downloads	Ratings	Reviews (2023)	Version
1	Period Tracker	H+F	Amila	mHealth	06-07-2015	4815692	211053	121	1.2.32
2	Pregnancy Tracker	P	Amila	mHealth	04-05-2016	6959308	353457	784	1.3.7
3	Ovulation Calendar & Fertility	P	Arbor Ltd.	mHealth	16-08-2018	4560286	43787	161	1.036
4	Pregnancy App & Baby Tracker	P	BabyCenter	FemTech	11-03-2011	29843944	1372090	1432	1.1.18
5	Clue Period Tracker & Calendar	H+F	Biowink GmbH	FemTech	09-10-2014	46252271	1172284	1532	117.0
6	Flo Ovulation & Period Tracker	H+F	Flo Health Inc.	FemTech	12-04-2016	104312618	2972261	3372	9.30.2
7	Period Tracker	H+F	GP International	mHealth	07-10-2011	23021300	359880	143	12.0.11
8	Grace Health Period Tracker	H+F	Grace Health	FemTech	03-11-2020	1485015	20719	150	2.21.1
9	Ovulation & Period Tracker	H+F	Leap Fitness	mHealth	29-09-2017	25253206	415931	559	1.093
10	Period Tracker	H+F	MeetYou	Unknown	21-02-2022	21611005	85724	1176	3.6.0
11	amma Pregnancy & Baby Tracker	P	Amma	FemTech	25-05-2015	13958191	332042	115	3.25.1.5
12	Pregnancy + Tracker App	P	Philips Digital UK	mHealth	28-01-2013	38210623	2177118	731	5.21
13	Premom Ovulation Tracker	H+F	Premom	FemTech	29-09-2017	1602247	10308	129	1.32.0
14	Ovulation Tracker & Calculator	H+F	Sadi Tech	FemTech	05-03-2021	1902002	11127	114	1.5.27
15	Period Calendar & Tracker	H+F	Simple Design	Generic	16-03-2012	173401566	5875562	2054	1.746.284
16	My Calendar	M	SimpleInnovation	Generic	16-08-2015	18789400	416860	582	8.5.6
17	Stardust: Period Tracker	H+F	Stardust App Inc.	FemTech	27-06-2022	65878	2122	240	2.14.0
18	Pregnancy Tracker	P	Timskiy	FemTech	07-08-2019	1652328	58475	412	3.90.0
19	Clover Period Tracker	H+F	Wachanga	mHealth	27-08-2018	4354982	154043	179	4.9.1
20	Pregnancy and Due Date Tracker	P	Wachanga	mHealth	16-08-2016	5807151	140653	221	1.1.18

H+F = Health and Fitness. P = Parenting. M = Medical.

APPENDIX B: USABILITY INSPECTION HEURISTICS

Table B.1: Summary of Privacy-by-Design guidelines [8, 15].

Guideline	Description
Data Minimisation	Data collection should be limited to only what is needed for provision of the service.
Anonymisation	Where possible, the user should not be required to submit data that could directly identify them, such as their real name, email address, or photograph.
User Control	The user should be able to give active and informed consent to collection and processing of their data, and should be able to opt out later.
Privacy Settings	Privacy settings should be available within the app, and should be flexible and user-friendly. Default settings should be privacy-preserving.
Right to be Forgotten	Data subjects should be able to request that all personal data be removed from the provider's systems.
Access and Correctness	There should be mechanisms for accessing past data and fixing it if incorrect.
Functionality	The application should not artificially restrict the service unless personal data is provided; e.g., app does not run without accepting all permissions, only real names allowed, and so on.
Transparency	The user should be provided with information about how their personal data is processed, and the reasons for processing before they enter sensitive data into the app.

Table B.2: Nielsen's ten usability heuristics [70].

Heuristic	Description
Visibility of System Status	Users should be kept informed about what is happening, through clear and timely feedback.
Match between System and Real World	The design should use words, phrases, and concepts **familiar to the user** rather than jargon.
User Control and Freedom	Users should have clear options for undoing behaviours and errors.
Consistency and Standards	Users should not have to wonder whether different words, situations, or standards mean the same thing.
Error Prevention	Errors should be prevented from occurring wherever possible.
Recognition over Recall	Options should be visible, and designs should avoid making users memorise or remember information.
Flexibility and Efficiency of Use	Designs should implement shortcuts for expert users, which can be hidden from novice users.
Aesthetic and Minimalist Design	Interfaces should not contain irrelevant or excessive information.
Recognise, Diagnose, and Recover from Errors	Error messages should be expressed in plain language, precisely indicate a problem, and constructively suggest a solution.
Help and Documentation	Where necessary, users should be provided with documentation to help them understand how to complete their tasks.

APPENDIX C: PRIVACY POLICY ANALYSIS CODEBOOK

Table C.1: Full codebook used in our analysis of female mHealth app privacy policies.

Code Name		Code Description	Example Data
Policy Scope	Single app	Policy only addresses the app being analysed.	*This policy applies only to information we collect in our App or through communications in relation to our App.*
	Multiple apps	Policy addresses the app being analysed in addition to other apps or services by the developer.	*This Privacy Notice applies to personal data processed by the apps, which are controlled by Philips and its affiliates.*
	No relation	Policy bears no relation to the app being analysed.	*The terms of our "Privacy Policy" apply to our website.*
Policy Version	Last Updated	The date on which the privacy policy was last updated.	*This Privacy Policy was last updated on December 4th, 2019.*
	Future Updates	Disclaimer that the privacy policy may change in the future.	*This Policy may amended to reflect changes in our practices with respect to Processing your information, or changes in applicable law. We encourage you to regularly check this page to review any changes we might make.*
User Data Types	App interaction data	Data relating to a user's activities or interactions while using the app, such as in-app search histories and clickpaths.	*We collect the information of your interactive behaviours, such as browsing, clicking and interacting with content.*
	Device and network data	Data relating to a user's device or network, including the IP address, device make and ID, cookies, etc.	*Automatically Collected Data may include device ID, advertiser ID, and device specifications such as display, model, OS.*
	Personal data	Data which directly relates to an individual, and can be used to identify them.	*When you sign up to use the Services, we may collect Personal Data about you such as your name, email address, and place of residence.*
	General health data	Data relating to a user's general health and wellbeing excluding their sexual and reproductive health.	*When you sign up to use the Services, you may choose to provide Personal Data about your health such as your weight and height.*
	Sexual and reproductive health data	Data relating to a user's sexual and reproductive health.	*We collect health data such as menstrual cycle, symptoms, and other information (including sexual activities).*
	Location	A user's geographical location, either precise (<1km) or approximate (city, wider region).	*The app uses Cookies to collect information about your IP address and location.*
	Audio-visual data	Photo, video, and audio data.	*If you add a picture to your profile, the apps require permission to access your mobile device's camera or photo gallery.*
	Financial data	Data associated with the user's bank account or financial transactions.	*If you pay for our Services, we may receive information and confirmations, such as payment receipts, including from app stores or other third parties processing your payment.*
Data Collection Methods	User input	Data is collected from the user via direct input; e.g., they enter the date of their last period.	*When you use our Service or perform certain actions, such as requesting services or information or contacting us directly, we may ask you to provide user information.*
	Device data	Data is automatically extracted from the user's device and/or its resources (e.g., camera, sensors, GPS, etc.).	*When you use Premom, we will automatically collect attributes such as the operating system and MAC address.*
	Cookies and interaction logs	Data is collected from cookies or other tracking technologies such as web beacons and app interaction logs.	*We collect Information through the use of cookies, eTags, Javascript, pixel tags, device ID tracking, anonymous identifiers and other technologies about (i) your visits to, and interaction and engagement with, the Services [...].*
	Third-party apps	Data is imported or collected from third-party apps or platforms, such as Facebook, Google, or Instagram.	*You can import Data from services such as Apple HealthKit and Google Fit such as sports activities, calories burnt, heartbeat, number of steps and other information about your health.*
Purposes for Data Processing	Service provision	Data is processed to provide and support core app functionality; e.g., IT and technical operations, in-app features, and security functions.	*We use data to deliver the services and products that you have requested, including storing information and files you provided to us for storage for the purpose of the Services.*
	Scientific research	Data is processed for research in partnership with clinical, academic, or scientific entities.	*To advance scientific research on menstrual and reproductive health, we share data with carefully vetted researchers to advance female health studies.*
	Analytics for app development	Data is processed for developer product research, to support, improve, or develop the app's features.	*The other reason why we process this data is to help us understand your needs and your use of our products, to analyze bugs and fix issues, and to bring you more useful features.*
	Analytics for personalisation	Data is processed for the purposes of tailoring app content to individual users.	*You can personalize your experience by adding health data into your profile. We will use this data to personalize Services, track your symptoms, and display articles of interest to you.*
	Advertising	Data is processed for the purposes of advertising, marketing, or commerce, in the app or across other websites and services.	*We provide advertising based on your interests and interactions with the Services and Channels.*
	Legal compliance	Data is processed in order to comply with a legal obligation, contract, or lawful request for access/subpoeana.	*We share information with law enforcement agencies, public authorities, or other organizations if we're required by law to do so or if such use is reasonably necessary.*
	Other	Any other reason for processing data.	*We may contact you to obtain customer feedback.*

Code Name		Code Description	Example Data
Data Storage/Retention	Data storage location	Description of where user data is stored; e.g., local device storage, company server, third-party server and its geographical location if applicable.	*Clue uses servers located in the European Union to process and store your personal data.*
	Retention period	The period of time for which user data is retained.	*We will retain Automatically Collected information for up to 24 months before storing it in aggregate.*
	Other retention period	Any other policies governing the storage and/or retention of user data, such as exceptions and special cases.	*If you choose to delete the App from your device or your account becomes inactive, we will retain your Personal Data for a period of 3 years in case you decide to re-install the App.*
Data Transfers	Data transfer to a third-party	Mention of user data being transferred to a third-party entity (to be cross-coded where necessary).	*We share your app usage information, such as analytics and unique identifiers, with our Advertising Partners who help us show you content and advertising in the app.*
	Cross-border data transfer	Mention of user data being transferred across international or state borders.	*Flo transfers Personal Data from the EU, EEA and UK to the U.S. and other third countries.*
Data Safeguarding Measures	Organisational	Measures which are carried out within organisations, such as due diligence, vetting of third-party vendors, and conducting risk assessments.	*Our security and privacy policies are periodically reviewed and enhanced as necessary, and only authorized individuals have access to the information provided by our users.*
	Technical	Measures which are technical and security-focused, such as encryption of data in transit and at rest, network firewalls, and anonymisation of data.	*In certain instances we may use Secure Sockets Layer encryption and/or transfer certain User Information in a non-human readable format to provide protection.*
	Limitations	Mentions of any limitations of the developers' data safeguarding mechanisms, or transferring of responsibility for security and privacy to the user.	*Although we take great efforts to protect your information, no security system can prevent all potential security breaches. We have no control over, and are not responsible for, the privacy practices of third parties.*
Regional Privacy Legislation	European Union (EU)	Policy references GDPR and other EU-based privacy frameworks, including the UK Data Protection Act (DPA).	*For EU residents' Personal Data we make reasonable efforts to ensure that such third parties are GDPR compliant.*
	California	Policy references CCPA, COPPA, and other Californian privacy laws.	*The California Consumer Privacy Act (CCPA) provides certain rights for California consumers. If you are a consumer residing in California, the following additional terms apply to you.*
	Cross-border laws	Policy references laws that regulate the transfer of personal data across international boundaries; e.g., Privacy Shield, standard contractual clauses.	*Everyday Health, Inc. participates in and has certified its compliance with the E.U.-U.S. Privacy Shield Framework.*
User Privacy Rights	Right to access and notice	The right of a data subject to know what data is held about them, and to access this data.	*You have a right to access your Personal Data you insert into the App and ask us about what kind of Personal Data we have about you.*
	Right to data rectification	The right of a data subject to correct or rectify inaccurate data that is held about them.	*If you believe that your Personal Data is inaccurate, you have a right to contact us and ask us to correct such Personal Data.*
	Right to data deletion	The right of a data subject to request that personal data held about them is deleted.	*In some circumstances, you may have the right to request that we delete any Personal Data which we have collected from you.*
	Right to data portability	The right of a data subject to receive their data in a common machine-readable format.	*Receive the personal data concerning you which you have provided to us, in a structured, commonly used and machine-readable format.*
	Other rights	Any other privacy rights afforded to users.	*The right to not be subject to a decision based solely on automated decision making, including profiling, where the decision would have a legal effect on you or produce a similarly significant effect.*
	Mechanisms for exercising rights	The channels by which a user can exercise their privacy rights, and the developer's process for complying with a request.	*You may contact us at help@pregnancytracker.app. For your protection, we may only implement requests with respect to the personal data associated with your account, and we may need to verify your identity before implementing your request. We will try to comply with your request as soon as reasonably practicable.*
	Consequences of exercising rights	Any unavoidable outcomes or consequences of the user exercising their rights; e.g., not being able to use certain features or services.	*Please note that if you make use of (some of) your choices and rights, you may not be able to use, in whole or in part, our Services anymore.*
	User consent	Mentions of user consent; e.g., mechanisms for gaining consent, use of consent as a legal basis for processing.	*By accepting this Privacy Policy you give PT your express consent, in your own power and for your own benefit, to the processing of your personal data in accordance with the conditions set forth in this Privacy Policy.*
Language and Readability	Ambiguous language	Language that is unclear or vague; e.g., vague use of conditionals/temporal adverbs without giving details.	*Also we send some information to our third parties. So your data may leave your country as our third parties may have their servers in different regions like Northern America, EU or Asia.*
	Contradictory language	Information that is conflicting or contradictory, either within the policy or when contrasted with Data safety sections and app features.	*We do not request and we ask you not to provide, including not to send us or disclose, any sensitive personal data.*

Code Name		Code Description	Example Data
	Complex language	Overly complex or technical statements, and jargon that is unlikely to be understood by a lay user.	*We use your personal data to fulfill the contract with you to provide you our Services per your request and consent prior to entering in the contract when signing up for our Services.*