“I don’t think it needs to be political”: Privacy Experiences and Concerns of FemHealth App Users in the United States

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

Alisa Frik
ICSI
afrik@icsi.berkeley.edu

Lisa Malki
University College London
lisa.malki.21@ucl.ac.uk

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

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

Abstract

FemHealth apps have rapidly developed, offering innovative opportunities to track users’ menstrual cycles, fertility, pregnancy, and other aspects of sexual and reproductive health. However, such apps collect a significant amount of sensitive user health data, posing privacy risks to users. In this paper, we conducted 14 in-depth semi-structured interviews with current and past users of FemHealth apps in the US to examine their privacy experiences and concerns. We found that participants were concerned about a wider range of risks than was found in prior user research about FemTech, including criminalization related to abortion or contraceptive access; emotional distress related to social stigma; third-party data sharing; and targeted advertising based on processing sensitive health data. Some participants acknowledged that FemHealth apps posed privacy risks and potential harms to users in general but were not necessarily concerned about their own privacy due to privilege (e.g., living in a state with strong reproductive health rights). However, all participants agreed that user privacy and data protection in FemHealth apps should be considered a fundamental right, not subject to legal discourse in specific locales. Most participants felt unsure about the effectiveness of existing data protection regulations and their interplay with anti-abortion laws. Participants suggested several ways to mitigate privacy risks, including disclosures and controls, back-end technical protections, behavioral strategies, and policy improvements. We provide recommendations for extending practical and policy-based privacy protections of sexual and reproductive health data collected by FemHealth apps.

Keywords

Privacy, FemTech, Mobile Health Apps, Female Health apps

Proceedings on Privacy Enhancing Technologies YYYY(X), 1–24
© 2026 Copyright held by the owner/author(s).
https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

FemHealth apps[1] (such as period, fertility, and pregnancy trackers) are part of a rapidly growing technology industry and are estimated to have more than 200 million downloads worldwide [25, 78]. They offer convenient and cost-effective access to services supporting health and well-being through a variety of features such as monitoring menstrual cycles, symptoms, and sexual activity; helping achieve or avoid pregnancy; and offering community support [78]. Such apps have individual, societal, and economic benefits [47, 49, 50]. They have the potential to empower FemHealth app users to better manage their health, narrow the gender health gap, and improve health equity and affordability [30].

However, to provide these functionalities, FemHealth apps collect sensitive data about users’ reproductive and sexual health, contact details, geographic locations, app interactions, browsing patterns, and other personally identifiable information (PII) [64]. By analyzing this data, apps can infer sensitive details, such as health conditions, sexual orientation, and political or religious beliefs, potentially exposing users to substantial risks of privacy harms [67, 69]. For example, inferences can be used for search engine optimization [64] and, as argued by some position papers, targeted advertising or discrimination [39]. In addition, the 2022 overturn of *Roe v. Wade* in the United States (US) [2], which ended the federal right to abortion, triggered significant concerns about “intimate surveillance” [60], in which sensitive data is harvested and commercialized at the expense of user privacy, catalyzing widespread fears and risks of criminalization related to abortion access [66, 77]. As a result, some users decided to delete their apps, and only a few felt empowered to take action beyond that [16]. Therefore, while FemHealth apps have the potential to empower users in managing their health, they can also pose privacy threats.

Various studies have analyzed the privacy risks posed by the use of FemHealth apps, including analyzing app privacy policies and data safety sections [64], public statements from app companies [85], and app reviews [72]; performing privacy-focused usability inspections [64]; conducting user surveys [16], and analyzing network traffic [84]. Most relevant to our work, Mcdonald and Andalibi [66] have conducted interviews with 15 participants who were pregnant or could become pregnant, sampling people residing in US states where abortion was legally restricted or criminalized. Their

[1] We use the term “FemHealth apps” for simplicity and consistency with how these technologies are referred to in the FemTech industry. However, we understand that the term may not fully represent the diversity of FemHealth app users, as these apps can be used by anyone assigned female at birth (regardless of gender).

study has explored participants' privacy threat model in a post-Roe world, with a particular focus on the risks of surveillance and policing of pregnancy (considering any type of technology rather than focusing on FemHealth apps). Moniz et al. [70] have also explored user views on intimate data and their self-protective strategies, using a Story Completion Method with four hypothetical scenarios related to various types of intimate digital health technologies (e.g., digital platforms used to track HIV status).

In contrast, our research specifically focuses on *FemHealth apps*; we include participants from US states with varying legal positions on reproductive rights; and we go beyond the risks of criminalization related to abortion access to explore broader privacy concerns, risk mitigation strategies, privacy information seeking behaviors, and views on relevant regulations. We discuss these differences in more detail in §2.2.

To this end, we address the following research questions (RQs):

- **RQ1:** What privacy risks associated with FemHealth apps are participants aware of and concerned about?
- **RQ2:** What strategies do participants employ (or would like to employ) to address or mitigate privacy risks?
- **RQ3:** How do participants seek information about privacy and data practices of FemHealth apps?
- **RQ4:** What are participants' views on the implications of data protection laws and privacy regulations with regard to FemHealth apps?

To answer our RQs, we conducted 14 in-depth semi-structured interviews with current/past users of FemHealth apps residing in the US. Participants considered data related to FemHealth to be highly sensitive, and they often viewed privacy in FemHealth apps as more important than in non-health apps because of the sensitive and personal nature of the data. Participants linked app features to privacy risks. For instance, location tracking was linked to an increased risk of criminalization, stalking, and harassment. Participants also voiced concerns over FemHealth apps selling data and using it for marketing, and psychological harms and stigmatization resulting from potential privacy and security breaches. Participants mentioned various ways to mitigate privacy and security risks, including user-facing privacy disclosures and controls, back-end data protections, and behavioral strategies. Trust in government-provided information resources and in the apps' own sources of information about FemHealth apps' privacy and data practices varied across participants. Most participants lacked confidence in their understanding of existing legal and regulatory protections. They suggested several practical, design, and regulatory improvements, including expanding current legal privacy protections like the Health Insurance Portability and Accountability Act (HIPAA) to consumer-oriented FemHealth apps, regulating the collection of FemHealth app data, and restricting access to FemHealth app data by third parties and government agencies.

Our paper makes the following contributions:

- It addresses gaps in previous research (as discussed in §2.2), and provides rich empirical evidence about FemHealth app users' privacy experiences and concerns, going beyond the risk of criminalization related to abortion access to consider broader privacy risks and other potential harms.
- It proposes novel recommendations for researchers, FemHealth app designers/developers, app stores, and policymakers to improve the privacy of FemHealth app users.

2 Background and Related Work

Here, we discuss previous work that has highlighted significant privacy and security risks associated with FemHealth apps, and users' privacy and security perceptions of them.

2.1 Data Practices in FemHealth Apps

FemHealth apps offer valuable tools for tracking reproductive health that bring a variety of benefits to users [28, 47, 49, 50, 78], while also raising significant privacy risks due to their handling of sensitive personal data [69]. FemHealth apps often share large amounts of personal data with third-party companies, libraries, and Software Development Kits (SDKs) [32]. Despite this, among the top 50 FemHealth apps, only one was classified as a covered entity under HIPAA, complied with its definition of "protected health information", and was required to comply with HIPAA requirements [36]. The lack of HIPAA coverage for many FemHealth apps means that most operate in a legal gray area, where sensitive FemHealth app data is not held to the same regulatory standards as comparable medical records maintained by hospitals and, therefore, are not protected or used as users would expect in a traditional healthcare setting[36, 83].

Furthermore, many FemHealth app privacy policies frame data protection as the responsibility of users (e.g., regularly checking updates), rather than developers and other stakeholders in the FemHealth app ecosystem, raising concerns about each stakeholder's ability to exert control over personal data [64]. However, the ability to protect one's privacy depends on users' understanding of app data practices, the risks such apps pose, as well as the protection strategies available to them. Nevertheless, similar to other genres of apps, privacy policies in FemHealth apps lack transparency and have poor readability, resulting in users having limited awareness of how these apps collect, store, use, and share their personal and sensitive data [35, 84]. Results from a focus group study with fertility tracker users have highlighted a perceived lack of transparency and control across these trackers, including apps, wearables, thermometers, and hormone monitors [48]. Many privacy policies of these trackers insufficiently explained how they handled sensitive user data, even when this was a core aspect of the tracker's service and functionality [84]. According to media reports, Flo—one of the most popular FemHealth apps—recently settled Federal Trade Commission (FTC) allegations and class-action lawsuits for sharing users' sensitive health information (e.g., pregnancy status, mood, and sexual activity) with third parties such as Meta and Google, despite assurances in its privacy policies that such data would remain private [3, 21].

Despite diverse sensitive data being collected, FemHealth apps often choose the "take it or leave it" approach to obtaining consent, in which users have no choice but to accept all terms to use the apps [67]. Beyond health metrics, FemHealth apps were found to track behavioral and location data, but only half of the apps included in the analysis requested explicit consent from users to collect such data [4]. Furthermore, FemHealth apps can collect data that goes beyond the individual user, including information about partners (in case of logging sexual activity), or children (for pregnancy and nursing tracking), resulting in uncertainties regarding data ownership and the absence of a clearly defined "data subject" [5]. A recent usability inspection of privacy-related UI elements in FemHealth apps, combined with an analysis of their privacy policies, revealed inconsistencies between in-app privacy features and the information presented in the policies. The study has also revealed manipulative design patterns in how consent is obtained and how data deletion options are presented (e.g., "cascading consent" granting automatic approval to the policies of all third parties receiving user data from FemHealth apps, lack of granular opt-out settings, and complicated consent withdrawal processes) [64].

The overturn of *Roe v. Wade* [2], which removed federal rights to abortion in the US, sparked a new wave of research on FemHealth apps, with a strong focus on the risks of criminalization and law enforcement access to reproductive data. FemHealth app privacy policies explicitly mention that users' personal data can be disclosed to governments and law enforcement agencies if developers are subpoenaed [24, 55, 64]. This is especially concerning because seemingly benign data, such as menstrual cycles or heart rate, can be used (sometimes incorrectly) to infer sensitive health statuses or reproductive choices [6, 64]. Despite critical legal repercussions, only a few FemHealth apps issued public statements addressing the *Roe v. Wade* overturn, and many apps continued to collect sensitive and personally identifiable data such as login credentials, demographics, IP addresses, and geographic location that could be used in legal cases related to seeking abortions [24, 85]. Although some apps have updated their privacy policies in response to the changing legal landscape of reproductive rights (e.g., by acknowledging the unique risks associated with FemHealth data, allowing users to delete data from app servers but retain it on their phone, and introducing new anonymity features), many have not [55].

In addition, existing privacy regulations in the US vary across states and are often criticized by position papers and law articles for their limitations, such as the absence of requirements for government access to data or the ease with which authorities can obtain data from third-party companies, leading to confusion among FemHealth app users and violations of their reasonable expectations of privacy [73, 79]. In the European Union (EU), the UK, and Switzerland, FemTech-related regulations are also inadequate to address the complexities of FemTech data practices [69]. For example, medical device regulations in the EU and the UK do not explicitly address the protection of FemTech data. Although GDPR offers certain privacy safeguards and requires explicit user consent for data sharing and processing, research demonstrates various challenges with comprehension and usability of user consent mechanisms [93], and practical difficulties in revoking consent [76].

Due to gaps in current regulations, unethical app data practices, and the broad range of potential data recipients, FemHealth app users face risks beyond criminalization, including loss of individual control, stigma, discrimination, targeted advertising, harassment, and domestic violence, as discussed by recent position papers [9, 39, 60, 77]. For example, according to media reports, employees may face adverse actions due to their sexual or reproductive health decisions, such as using birth control or undergoing fertility treatments [71]. Advertisers could leverage location data to infer reproductive health status based on visits to fertility or abortion clinics, further increasing "surveillance capitalism" [22, 77] and "intimate surveillance" [60]. Thus, privacy risks posed by these apps extend *beyond* political contexts to include broader dimensions of harm that impact users' autonomy, safety, and well-being.

2.2 FemHealth App Users' Privacy Concerns

Prior to the *Roe v. Wade* overturn [2], FemHealth app users did not often discuss privacy or security issues, viewing the data shared with these apps as rather uninteresting and unproblematic [7, 13, 38, 46, 59]. However, there were several exceptions. In a mixed-method study, participants who used menstrual trackers were concerned about social stigma and, therefore, considered app reminders and notifications that could be seen by others as privacy violations [91]. Although participants in another study believed that no individuals or organizations would be interested in their menstrual app data, a small number expressed discomfort that their data could be shared for targeted marketing [46]. Non-users of period-tracking apps were more likely to criticize these apps for perceived privacy issues, compared to those who actively used them [7]. Participants who expressed concerns proposed some risk management strategies, including data minimization or choice of "credible" apps, while others approached privacy issues with a sense of resignation or a trade-off between privacy and utility.

In contrast, there has been a growing body of research focusing on users' privacy concerns in relation to the risks of criminalization, following the overturn of *Roe v. Wade.* A survey of 183 US-based participants across states with differing abortion policies has examined period-tracking app users' privacy concerns [16]. Although participants did not fully grasp the impact of the *Roe v. Wade* overturn on their reproductive privacy, they were concerned about law enforcement access to their data, and felt uninformed and powerless to address these privacy risks. In a study with UK-based participants [68], while FemTech data was viewed as highly sensitive, participants lacked awareness of how FemTech operated, who had access to the data they collected, and what legal rights users possessed. Participants expressed significant concerns about privacy risks, including the possibility that their data may be sold or shared to third parties and governments. The perceived sensitivity of personal data collected by period- and fertility-tracking apps has also been demonstrated in qualitative work [87]. A recent study has explored how Reddit users collectively contextualize privacy issues and speculate about associated risks (e.g., prosecution, surveillance, harassment, mental health implications) with respect to period and fertility trackers [86]. The study has also explored the ideas suggested by Reddit users to mitigate such privacy risks, including stopping the use of period and fertility trackers, choosing European-based trackers, providing deceptive health data, and voting for political candidates supportive of reproductive rights. Changes in user sentiment are also reflected in app store user reviews. A recent analysis of user reviews available in the Google and Apple App Stores has shown that FemHealth apps received mainly positive feedback until 2022, after which the reviews became predominantly negative [72]. Privacy concerns among users in the reviews were identified as a key factor behind the decline in sentiments, with an increase in comments referencing *Roe v. Wade* overturn and issues related to data processing.

These privacy and security concerns influenced the behavior of users of menstrual cycle (MC) tracking apps [80]. Many pre- and peri-menopausal users reported stopping using MC apps optinginstead for non-app-based tracking methods due to the shifting legal landscape; and some choosing not to participate in FemHealth app research for the same reasons [80]. A recent study involving interviews with 15 US participants who were pregnant or could become pregnant—and who resided in states where abortion had been made illegal or restricted—examined participants' privacy threat models in the context of digital technologies more broadly, without specifically focusing on FemTech-related tools. The study has revealed how most participants deleted their FemHealth apps after the overturn of *Roe v. Wade.* Participants with lower-risk profiles (e.g., being older or living in non-restrictive states) employed no or low-technology privacy strategies (e.g., avoiding abortion clinic searches) and those with higher risk used a combination of no/low-technology and high-technology strategies (e.g., using Virtual Private Networks (VPNs)) [66]. In Australia, privacy and security concerns have also created a significant barrier to using pregnancy apps among pregnant participants [58]. In contrast, insights from interviews with US-based teenage participants showed that many continued using period-tracking apps despite being aware of potential privacy concerns [23]. Many teenage participants believed that they were at a reduced risk of pregnancy—and consequently less likely to be prosecuted for abortion—due to not being sexually active or not engaging in heterosexual relationships. Another study (still a pre-print during the writing of this paper) has analyzed mobile app usage patterns before and after abortion bans, finding a "chilling effect" with FemHealth app usage dropping after the *Roe v. Wade* overturn verdict leak [10]. In addition to self-reported disengagement from FemHealth apps, there was a notable increase in the use of privacy-preserving browsers, accompanied by a significant decline in both the frequency and duration of FemHealth app usage following the overturn of Roe v. Wade.

Gaps in prior work. Although previous research has provided important insights, there are still significant gaps in our understanding of FemHealth app users' privacy concerns and lived experiences. First, several existing studies relevant to our research have examined the perspectives of users located outside the US [48, 57, 68], or have focused on examining the views of US-based users living in states where abortion access is restricted or criminalized, with a specific focus on how these views were influenced by legal bans after the overturn of Roe v. Wade, thus overlooking other potential harms [16, 66]. Secondly, many existing studies have focused on broader categories of female-oriented technologies or on the privacy of reproductive health data more generally, rather than specifically examining FemHealth apps [23, 66, 68]. Third, many studies have used quantitative and mixed-methods approaches, with qualitative insights being limited to open-ended survey questions or secondary analysis of user reviews [16, 24, 72, 80]. Finally, some work has focused on specific demographic groups and user populations, such as pre- and perimenopause participants [80] and teenagers [23]. For detailed information on how our study compares to prior work, see Table 1 in Appendix B.

Our in-depth interview study, involving a diverse group of current and former FemHealth app users in the US—spanning various ages, ethnic backgrounds, privacy concerns, and residing in states with differing reproductive rights laws—seeks to fill key gaps in existing research. By providing rich qualitative data, the study sheds light on a wide range of privacy concerns, users' strategies for mitigating risk, and their behavior when seeking privacy-related information. This empirical evidence supports the development of more privacy-aware FemHealth apps that users can benefit from rather than abandon and guides policy decisions related to digital health and reproductive privacy.

3 Methods

Our study followed the ethical principles outlined in the Menlo Report [51]. We provided participants with study details, obtained their informed consent, and allowed them to skip questions or withdraw at any time. The Research Ethics Committee at our institution also approved our study.

3.1 Participant Recruitment

To be eligible to participate in the study, participants had to be current or past users of FemHealth app(s) designed to track menstrual cycles, fertility, pregnancy, and other areas of sexual and reproductive health; reside in the US; and be fluent in English. We created a screening questionnaire to capture participants' use of FemHealth apps, demographics (e.g., age, gender identity), technical knowledge, and privacy awareness (see Appendix §A.1). The screener was administered using the survey platform Qualtrics, and participants were recruited via Prolific, a crowd-sourcing platform. A total of 200 respondents completed the screener. We excluded 51 respondents for never having used a FemHealth app. We then used purposive sampling to to include participants with diverse demographics (e.g., ethnicity, age, gender identity), varied experience with FemHealth apps (i.e., roughly equal numbers of current and former users), and different levels of privacy concerns. We also aimed to recruit a diverse sample of participants from across the US, including states with varying legal landscapes on abortion—ranging from those where abortion was banned to those where it remained legal up to the point of viability.

3.2 Data Collection

We conducted 14 in-depth semi-structured interviews. Five HCI and privacy researchers reviewed the screener and interview guide, and two additional researchers reviewed the final materials. We iteratively refined the materials based on their feedback and input from three pilot participants. We included pilot data in the analysis as no major changes in the interview protocol were made. We then conducted nine interviews between March and May 2024, and two additional interviews in September 2024 to confirm we achieved data saturation across our purposively selected sample.

Our interviews began with introductory questions about the general experiences of participants using FemHealth apps. We then explored their beliefs and feelings related to the data practices of the apps they were or had been using, views on and experiences with data deletion mechanisms, their privacy concerns, the sources they relied on for information or advice about privacy in FemHealth apps, and their opinions on app stores' privacy nutrition labels (i.e., the Data Safety sections in Google Play for Android apps and the App Privacy sections in the Apple App Store for iOS apps). However, because the insights related to privacy nutrition labels were not novel compared to previous work [e.g. 52, 61, 88], we do not report them in this paper. We then explored participants' experiences with and preferences for strategies to mitigate privacy risks, and views on the implications of existing privacy regulations on FemHealth apps. Finally, we asked participants about the desired improvements in the technical and regulatory protections of FemHealth apps. (See the interview script in Appendix §A.2.)

Our interviews lasted between 1 and 1.5 hours and were conducted via video chat using an institutional Microsoft Teams account without collecting participants' IP addresses or requiring users to login. Interviews were recorded, and automatically transcribed using Microsoft Teams. Participants were compensated $38 USD each (equivalent to $30 per hour, based on the average duration of an interview), which reflects common compensation practices in qualitative user research, and was deemed appropriate without introducing the risk of coercion by our ethics review committee. The first author, who conducted the interviews and participated in data analysis, manually cleaned the transcripts to correct any errors, removed all names and personally identifiable information, and assigned anonymous participant IDs to ensure participant anonymity. We then stored anonymized transcripts on our institution's encrypted server and securely deleted all audio recordings, to protect participants' privacy.

3.3 Data Analysis

We thematically analyzed all interview transcripts. After familiarizing themselves with the data and taking notes, three researchers independently coded two interview transcripts (that were randomly selected) using MAXQDA, to develop an initial coding frame each. A combination of deductive and inductive coding was employed to analyze the qualitative data. High-level topics were guided by our RQs, while specific codes were developed from recurring patterns in participants' responses. They then discussed and merged their individual coding frames into one frame after resolving disagreements. Using the merged frame, they randomly selected and independently coded an additional transcript (different from the previous two), updating the coding frame as needed. After repeating this process for other transcripts, we concluded that no new codes were identified after coding the twelfth interview. We conducted and coded two more interviews, which also did not yield any new codes, suggesting that data saturation has been reached. Then, the same three researchers re-coded all transcripts using the finalized coding frame, ensuring that each interview transcript was coded by two researchers independently and continuing to discuss questions about code application throughout.

All three researchers then iteratively identified, developed, and refined themes by organizing codes into themes that were relevant to addressing our RQs and reviewing the corresponding excerpts for each topic to further refine the themes. The three researchers also discussed and resolved any coding discrepancies to provide reliable counts of theme occurrences, which we present in this paper as an estimate of theme prevalence in our sample. However, we caution the reader against interpreting these counts as quantitative findings, as the goal of our qualitative study is to illustrate the breadth of opinions and perspectives, and our sample size is not necessarily sufficient to draw statistically generalizable conclusions.

3.4 Limitations

As with most qualitative studies, our findings may not be generalizable beyond our sample. While our sample size is consistent with widely-accepted qualitative research standards [15, 37, 42, 81], which emphasize obtaining rich, contextualized understanding over statistical generalizability or quotas [94], and was sufficient to achieve data saturation and address our RQs, it may not accurately represent the broader US population. Furthermore, our sample did not capture the opinions of people under the age of 22, who can also use FemHealth apps [27] and may have different privacy concerns and risk profiles. However, we obtained a diverse sample of adult users across different ethnic backgrounds, privacy attitudes, sexual orientations, and prior experiences with FemHealth apps, as well as various (but not all) states of residence. Thus, our results reflect a variety of views. Drawing on our findings and related studies, future work could create a large-scale survey instrument to quantify these insights, identify statistically significant differences in views across socio-demographic factors, and facilitate comparisons across countries and states.

As with most self-assessment data, our findings may be influenced by social desirability bias [12]. To mitigate this risk, we ensured response anonymity and allowed participants to skip any questions. Future work could validate our findings through observational methods to further reduce this limitation and assess the accuracy of self-reported data. To minimize bias in question framing while allowing participants to express positive experiences and concerns, we asked about both positive and negative sentiments, as well as data practices they felt comfortable or uncomfortable with. The semi-structured interview format enabled tailored follow-ups to capture nuances in individual experiences and attitudes. Finally, given the personal and contextual nature of privacy, we did not impose a predefined definition; instead, we asked participants to define privacy in their own terms to guide subsequent discussion. The resulting variations in conceptualizations were minimal and do not undermine the interpretation of our findings.

4 Results

In this section, we present our study findings.

4.1 Participants

Participant demographics and experiences with FemHealth apps are described in Table 2 in Appendix C. Out of 14 participants, eight were current users of FemHealth app(s) and six were past users (four of whom discontinued their use due to privacy concerns). Ethnic groups included White or Caucasian (n = 5), Asian or Asian American (n = 4), Black or African American (n = 2), Hispanic or Latin American (n = 2), and Middle Eastern (n = 1). Participants' ages ranged from 22 to 46 years. Ten participants were heterosexual, three were bisexual, and one was homosexual. Most participants held a university degree, including six with a Bachelor's, five with a Master's, and one with a Doctorate. The majority of participants were either employed full-time (n = 9), part-time or causally (n = 2), or self-employed (n = 1). Most participants (n = 13) were women, and one was non-binary. In the survey, participants reported that they used or had used FemHealth apps for the following purposes: menstrual cycle tracking (n = 11), period predictions (n = 9), fertility or ovulation predictions (n = 8), sexual activity tracking (n = 4), mood and mental health tracking (n = 4), physical symptom tracking (n = 4), birth control management (n = 2), push-notifications and reminders (n = 2), and other (e.g., weight tracking) (n = 1).

4.2 Privacy Risks and Concerns (RQ1)

Participants mentioned a wide range of privacy/security risks, some of which, like **hacking and data leaks/breaches** (n=9), are common in various genres of mobile apps, while others are more unique to FemHealth apps. In this section, we focus on reporting the risks specific to FemHealth apps.

FemHealth data was perceived as sensitive. Many participants (n=10) found FemHealth data to be **sensitive**, deeply personal, and even *"intimate"* (P14). Participants noted that dates of menstrual cycles and symptoms can reveal information about a possible pregnancy, miscarriage, ovulation window, or FemHealth-related problems. Some participants mentioned that they used FemHealth apps to track their sexual activity, while topics related to sexuality were still considered a taboo in certain participants' communities, with premarital sex viewed as "a sin" (P4) in some religions.

Many participants (n=11) said that **privacy was more important in FemHealth apps** than in most non-health related apps, for example due to the personal nature of the data FemHealth apps collected, even if it was not formally classified as part of health records or granted the same protections: *"I feel like it's kind of a gray area because period data isn't necessarily part of your medical record or anything, but it is kind of sensitive because it's very personal"* - P5. Two participants thought that privacy in FemHealth apps was more important specifically due to the *"political climate of the United States"* (P8) around reproductive rights and potential criminalization risks (which we discuss in more detail later in this section). Two participants thought that although privacy in FemHealth apps was more important than in many other non-health apps, it was less important than in apps like those used for banking or social media—due to a belief that menstruation-related data could not reveal as much detailed information as the extensive content shared on social media. One participant also expected health-related data to be better protected by special privacy regulations like HIPAA than non-health-related data: *"There are actually more, like, privacy regulations with health data... Like the HIPAA compliance stuff which I don't know a lot about, but I know it's more limiting on privacy of health data"* - P2. Finally, some participants (n=4) believed that privacy may be equally important in FemHealth apps and non-health apps, as both could collect sensitive data.

The belief that FemHealth data is highly sensitive made participants especially uneasy about the possibility of companies profiting from its use by, for example, **selling** (n=11) or **sharing it with third parties** without users' explicit consent (n=6), or using it for **marketing purposes** (n=8): *"Just the idea of like someone who has to profit off of my personal data, my health data, using that against me, or to advertise to me just makes me really uncomfortable. I don't feel personal data should be used in that way and it feels like a violation of privacy"* - P3. Participants found that these practices were *"creepy"* and *"evil"* (P4) and did not *"feel right"* (P3).

About half of participants (n=8) **were concerned about location tracking** features in FemHealth apps. For two participants, this concern was linked to the fear of criminal prosecution, as location data could suggest that someone from a state where abortion is banned had traveled to a more permissive state, potentially implying they sought abortion: *"I am right now living in Ohio, which is one of the places where abortion is very, very limited, so you can be criminalized if you like, you know, travel to another state [to get an abortion] and they can track that through the app"* - P1, or might have visited an abortion clinic: *"They may want to know if I'm in the vicinity of an abortion clinic or anything so that, like I keep saying, they can criminally charge me"* - P10. Location tracking also raised concerns about **stalking and harassment** (n=3): *"People can use your information to, you know, locate you. So, if it ends up in the wrong hands, maybe like a stalker or something"* - P1.

Some participants (n=5) were concerned about potential **emotional distress or psychological harms** resulting from unintended disclosure of sensitive personal information collected by FemHealth apps: *"I guess, it wouldn't do any physical harm, but emotional damage ... if someone knows my period now, it feels kind of creepy. It feels weird. And maybe it caused me to kind of overthinking and worry about if there's some more people know my private data, like get a little bit paranoid"* - P5. In some cases (n=4), these mental health related concerns were associated with the risk of social judgment or stigmatization: *"In maybe more religious countries, if your information ends up online, even though it's not criminalized or something like that, you might be, you know, shunned from society or something like that"* - P1. Two participants speculated that the exposure of FemHealth app data in the workplace could *"affect them professionally"* (P7) or lead to **workplace discrimination**.

Criminalization risks. The most prominent privacy risk associated with FemHealth apps, mentioned by almost all participants (n=12), was related to **criminalization**, whereas data collected by FemHealth apps could be used to condemn or prosecute users of such apps. The most common example mentioned was related to enforcing anti-abortion laws. For some participants (n=4), the changes in reproductive health rights and legislation after the overturn of *Roe v. Wade* were the reasons for discontinuing the use of FemHealth apps: *"That was one of the reasons I also stopped using period trackers because in some states, abortion was being criminalized. Miscarriages as well. So, I was kind of not afraid, but worry about, like, if this data can be used to criminalize somebody"* - P1.

Some of the US state laws introduced restrictions not only on abortions but also on **access to contraceptives**. Since many FemHealth apps provide features for tracking the use of birth control methods, two participants saw these features as privacy risks that *"could be very harmful"* (P3). Some participants (n=4) acknowledged that although they were not presently concerned about risks related to abortion or contraceptive access, rapid developments in the political climate could change their views: *"Even though I don't have to necessarily worry about that right this second, it does worry me how they might turn to these apps to, you know, look for people"* - P14.

Unlike pregnancy-tracking apps that explicitly asked users to enter pregnancy-related information, period-tracking apps could *infer* such information. Some participants (n=5) were **concerned about information that can be inferred** without any user control over it. P12 was specifically concerned that such **inferences from FemHealth app data could be inaccurate or misinterpreted**—for example, when a missed or delayed period could be mistakenly attributed to an abortion rather than a miscarriage or hormonal imbalance: *"People could literally go to jail for having a miscarriage, which has happened in Texas. People have used that to send women to jail, claiming that it was an abortion, when the main basis of the evidence was a tracking app and not much else. So, people could lose their liberty and their freedoms unjustly because the information is not protected well"* - P12.

Many participants expected **cross-state** (n=9) and **cross-country differences** (n=13) in the privacy risks posed by FemHealth apps, influenced by varying social norms: *"For example, in Saudi Arabia or the Middle East, women don't have as many rights as in the US. So, if someone's data were breached over there and it showed activity like frequent intercourse or an abortion, it could result in severe punishment, like life in prison. ... But in America, it depends on the state—like you'd be fine in Colorado but might face serious consequences in Louisiana"* - P4. Two participants anticipated greater protections offered by FemHealth apps used in Europe due to the belief (not necessarily correct, see §5.3) that privacy regulations are stricter in Europe than the US: *"If I was in say the EU where, my impression is that there are better regulations about data privacy, I would feel more comfortable using this app than I do right now"* - P3. Almost half of participants (n=6) believed that the privacy of health data is a fundamental human right that should be universally protected regardless of the political climate or legal discourse in a given locale: *"I just think that's women's private information, and I don't think politicians need it. I think that's our health, and I don't think it needs to be political"* - P7.

Despite acknowledgign various privacy risks, almost all participants (n=13) were not actively concerned about their own privacy, for example, because they had not experienced a miscarriage, had not had an abortion, did not plan to have more children, had already entered menopause, lived in states with strong reproductive health rights and protections, or had not used FemHealth apps for years. Yet, even among those participants, some (n=4) were concerned about the impact criminalization could have on *other* people, including their own daughters: *"I've been thinking about the tracks of the apps a lot recently for my daughters because one is menstruating... both her doctor and I... We said get a notebook, keep it in the bathroom... I don't think I would encourage her to use apps now. I'm just too worried about what is out there"* - P11.

Legal risks were not always related to the use of data by governments. For example, as a single parent, P12 was concerned that information she tracked about her mood fluctuations throughout her menstrual cycles could be used against her in court by the biological fathers of her children in an attempt to gain custody: *"I do track moods and things like that because it is tied in with my menstrual cycle... I'm a sole parent... If they [fathers of my children] ... decide to take me to court and try and get shared custody... If they were to gain access to my mood data, they could potentially use that in court to show emotional instability"* - P12.

Privacy perceptions in paid vs. free FemHealth apps. Some participants (n=3) believed that privacy protections would vary between free and paid FemHealth apps. For example, P1 speculated that free apps might be more likely to sell user data as a means of monetization, while users of paid apps could expect stronger privacy protections in exchange for their subscription fees: *"They might be selling health-related data to pharmaceutical companies... because this app is free. ... Because they are using your information somehow to make profit... if you use an app that you paid for, that assures you that your data will be deleted... If I decide to use an app like that again, I think I would do it like that, like pay for privacy"*. In contrast, P13 believed that the additional features available in paid versions of FemHealth apps could result in more extensive data sharing compared to the free version of the same app: *"I also know that Flo, once you pay, also has access to connect with healthcare professionals. ... So, for sure, your data is going to be shared with the healthcare professionals that are going to be assisting you"*. Moreover, by paying for the app, P6 was worried to expose their financial information: *"They're always asking to buy the premium version, to pay for the app. I have heard things on social media about how data and things like this could be stolen... and so because of that, it does kind of limit the types of information I want to put into the app"*.

Are benefits worth the risks? In line with the privacy calculus theory [56], participants weighed the potential risks to their privacy against the benefits they received from using FemHealth apps. Some participants (n=3) concluded that, for them, the risks outweighed the benefits, particularly since they could track their menstrual cycles using alternative, more privacy-preserving methods, such as spreadsheets, offline calendars, or paper notebooks: *"They're not worth using. I can chart my information on a calendar... in the privacy of my own home, my own private calendar that won't be shared with anyone"* - P10. However, about half of participants (n=6) valued the convenience offered by FemHealth apps and had lower privacy concerns, or felt confident that the apps adequately protected their privacy. Yet, even among those who believed the benefits outweighed the risks, several participants *"felt resigned"* (P2) and lacked alternatives, as they believed that all FemHealth apps collected personal data: *"There were data leaks from female reproductive apps, such as, Clue, Flo... If all the apps were taking data, where would I go? So, I figured the benefits outweighed the cons, and I decided to keep using it"* - P6.

Some participants (n=4) thought the trade-off depended on the data practices or even brand of a specific FemHealth app, personal circumstances and preferences, perceived severity of and vulnerability to privacy risks, or the political climate in the place of residence: *"For Apple, I'm comfortable with it. I don't think that the privacy risk outweighs it. For several others I do though"* - P12.

Key findings: *Participants perceived the data collected by FemHealth apps as particularly sensitive due to concerns about potentially inaccurate inferences, workplace discrimination, and stigmatization related to fertility, pregnancy, miscarriage, and abortion; cultural taboos surrounding sexual activity information; and fears of criminalization.*

4.3 Risk Mitigation Strategies (RQ2)

Participants mentioned various strategies to mitigate privacy and security risks, including user-facing disclosures and user controls, back-end protections, and behavioral strategies.

User-facing privacy/security disclosures and controls. The first step in addressing privacy and security risks was increasing user awareness of these risks and how to effectively mitigate them. Indeed, many participants (n=10) mentioned the desire for greater **transparency and explainability** about app data practices (see also §4.4 for how participants preferred to learn about privacy and security). In addition to having clear explanations of data flows, participants were concerned about criminalization, wanted detailed information about whether and how FemHealth app data could be shared with government and law enforcement agencies. They also appreciated the reassuring tone adopted by some apps in their messaging and public commitments to user privacy: *"When I logged into Clue, they had a pop-up trying to reassure consumers or users that their data was secure and wasn't going to be sent out ... it was definitely needed to reassure women because I feel like a lot of women were definitely scared for their own reproductive rights and concerned over how much control they have over their bodies"* - P9.

Besides transparency, many participants **wanted to have a choice** — whether to provide informed consent or grant permissions (n=11), or opt out of certain data practices (n=5). Even when user data was going to be shared with presumably legitimate recipients for benevolent or legitimate purposes, such as sharing data with doctors providing app users with care, participants wanted to have granular control: *"I guess with my consent, I would feel comfortable with Flo sharing the information with my doctor, or something. I mean, an OB/GYN, not just an average doctor"* - P5. Participants stressed that the Terms of Service must be clear, concise, specific, and ideally backed by legal enforcement to be truly meaningful and informed, as well as indicated that consent must be revocable.

Half of participants (n=7) mentioned **privacy settings and user controls** as another privacy protection mechanism. However, they admitted that they did not engage with privacy settings much beyond the onboarding period when they first installed the app, if at all. Interestingly, P2 expressed a desire for the ability to hide sensitive FemHealth information on the Apple Health dashboard to avoid accidental exposure through shoulder surfing: *"So, in Apple Health there's this section of Favorites. ... it says 'oh you're fatigued and have cramps' or 'you had sex' ... I would like for some of those to be able to choose, for some of those things to not show up in the app screen on the Favorites... I don't want people to be able to see all that stuff if they're sitting next to me".* Two participants wanted **defaults to prioritize privacy**, proactively safeguarding FemHealth app users' privacy rather than placing the responsibility for protection on users: *"I feel like my privacy should be protected by them [app providers]. That should be the default setting. It shouldn't be my job to find out whether you are protecting my privacy"* - P5.

Additionally, about half of participants (n=8) mentioned the importance of **security features**, including strong passwords, app locks (e.g., requiring face recognition or a PIN to unlock the app), and two-factor authentication.

Back-end privacy/security protections. Participants mentioned several ways that apps could protect user privacy/security by changing the way user data was managed, including **anonymization** (n=6), **encryption** (n=5), and **data minimization** (n=4). Allowing participants to choose **pseudonyms** instead of real names was one way to limit tying data to personal identifiers: *"I could join with a pseudonym, hopefully without giving my real address, using a specific email address just for that purpose"* - P11. P2 suggested avoiding associating data not only with personal identifiers like names, but also with device identifiers: *"I would like them to make sure that the data cannot be stored and traced back to you, so I guess don't store the health data along with any identifying information or even I think, like, I don't know, the device's information".*

Behavioral strategies. Almost half of participants (n=6) mentioned **self-censorship**—limiting the data they provided to the app, or providing fake information—as a way to protect their privacy: *"If you are really concerned about like abortion issues or miscarriage issues, even though you don't get your period, maybe you can just enter it as if you've gotten it"* - P1. Although almost half of participants (n=6) believed that information they input into the app was all the data that the app collected, in reality, the app could also collect metadata and data from phone sensors or make inferences. This misconception led to underestimating risks: *"I think to me the risks are quite small, especially because I do select what kind of data goes into it"* - P6.

When participants had privacy or security concerns about the data the app had already collected about them, many of them (n=11) suggested to **stop using the app**, **delete the data** (n=6), or **delete the app** (n=6) to protect privacy. Many of these participants expressed a desire for a data deletion feature, preferably accessible directly within the FemHealth app's settings or on the company's website. However, they also expected those features to be *"hidden deep down in the account settings"* (P11) and difficult to find or use. Some participants (n=4) suggested that FemHealth apps should automatically delete user data on a regular basis, with guarantees that no copies or backups were retained, to enhance users' sense of ownership and control over their data: *"They could ensure that if you choose to delete your information, it really goes away. You know, giving the user a sense of security... They could verify if there's always a backup copy or not and just let us know. They could provide a quick link like, "If you want everything deleted, click here"... It should be easy to do that if you choose to"* - P8. Half of participants (n=7) said that if they were unable to delete the data themselves, they would resort to sending data deletion requests to app developers or customer service via email, though this methods was less preferred: *"I think I had to email Flo to have them delete my data. There was not a simple method to do it in the app, so I may have to do that with Clue as well. That's kind of a red flag—anytime I have to send an email to say, "Hey, can you delete my data?" Why can't I just easily delete it using the app?"* - P4. About half of participants (n=8) expressed a desire to save a copy of their data before deleting it, to retain information for potential future reference, recover their account, transfer data to a new app, migrate data to a new phone, or at least understand what data the app had collected and/or inferred about them and might have been shared with others.

> ***Key findings:*** *Participants wanted greater privacy transparency—particularly regarding data sharing with government and law enforcement agencies due to concerns about criminalization—along with more granular privacy controls (even when sharing data with healthcare providers) and discreet interface designs to prevent accidental disclosure of sensitive reproductive health information. In the absence of such protections, many reported considering discontinuing app use.*

4.4 Information Sources (RQ3)

This section discusses how participants sought information about FemHealth app data and privacy practices, and which information sources they trusted the most/least.

How participants learned about privacy. Half of participants (n=7) said they learned about data practices and privacy through the **information directly provided by their FemHealth apps**, including in-app content or notifications, apps' websites, privacy policies, FAQs, app store descriptions, and emails. These sources were used most frequently, as they required less effort to find than proactive **online searches** (n=3), including on government websites (n=1), on non-government websites (n=3), and in scientific research articles (n=1). Some participants mentioned learning about privacy in FemHealth apps through **media** (news (n=7), social media (n=4), podcasts (n=1)), and from **conversations with peers** (n=4). Information about data practices and privacy not only increased the awareness of many participants, but also increased their confidence in apps (n=9): *"It does make me feel good that... I didn't see anything that threw off any major alarms. I didn't see anything that scared me away. ... That experience right there gives me even more confidence in the fact that I made the right choice"* - P12.

What sources participants trusted the most/least. Some participants trusted well-known reliable news outlets (n=6), scientific articles (n=3), and information disseminated by independent organizations like NGOs (n=2). While almost half of participants (n=6) trusted national or international government organizations (e.g., WHO, NIH, Department of Health), two participants distrusted information shared by governments due to past breaches of trust, which had undermined their confidence in official sources (*"We've had issues, like with the pandemic, with government-sponsored websites having data that changes and may not be the most truthful... America doesn't have the best track record for health for Americans and especially minorities, so I probably wouldn't trust anything they put out"* - P4), or due to the politically charged climate surrounding reproductive health (*"Just because of the abortion fight in the United States. The laws in the United States—not just Texas, but all over—I just feel like the climate has changed quite a bit"* - P8.)

Participants had mixed feelings about trustworthiness of apps' self-disclosed data practices, with about half (n=8) saying they would trust apps' own disclosures and some (n=5) saying they would have doubts about them. While privacy policies could be legally binding documents, these participants suspected that companies could prioritize profit-seeking interests over fully honest and transparent privacy disclosures: *"I think I trust the companies' own like FAQ for their privacy policy, because the privacy policy I think is a legal thing. ... but I also kind of think they will probably say in a way that's beneficial to them or downplays anything people might perceive as being negative. So, I kind of take it with a grain of salt"* - P2. Although privacy nutrition labels (e.g., Google Play's data safety sections) were recently introduced to provide a concise summary of app data practices, almost all participants (n=12) did not recognize or recall reading such labels. All participants (n=14) also mentioned that some sections of these labels were contradictory or did not mention that data could be shared/used by law enforcement agencies and for what purposes.

The reputation, expertise, and trustworthiness of the specific person or organization sharing information were key factors influencing how some participants (n=4) perceived the trustworthiness of the information shared on social media. Thus, participants were often skeptical of the accuracy of such information and said they would *"take it with a grain of salt"* (P1). Some participants (n=3) said they would not trust any information about FemHealth apps' privacy found on social media. Yet, most participants (n=12) were willing to share privacy-related information about FemHealth apps they learned from peers or online forums and social media, particularly when the information raised privacy concerns and they were confident in its accuracy.

How participants preferred to learn about privacy. **Proactive disclosure** of information related to data practices and privacy in FemHealth apps was important for most participants (n=12): *"I think it would be best if I could hear about how they [apps] are taking better steps to protect my data rather than learning about it from social media or something"* - P6. The absence of that information in the app raised privacy and trust concerns, and led some of the participants to decide against using the app: *"If I can't find anything in the app, that would raise concerns because I don't think they're being transparent. ... I would definitely delete the app if I couldn't access that information in Flo"* - P13. Participants said that they wanted this information to be **clear, easy to discover and understand, concise, and upfront**. For example, P12 found health-related data to be especially important and sensitive, so she was disappointed when companies intentionally made it difficult to understand how this data was protected: *"They don't wanna make it easy on you. So, some of them, it's in the privacy practices and then some of them have it in the FAQs and some of them have it hidden in some other random area. So, it's a lot of digging to find the information which honestly is a little disheartening. You would think that for something health-related that it would be more upfront and easily accessible."* That participant (along with others) instead preferred the **privacy disclosures to be presented as early as during the download or sign-up process**. Since some participants did not trust the app's own communications about data practices, they wanted additional app store or independent third-party vetting to verify the app's privacy claims: *"I know that the Google Play store on every application says clearly whether an application sells your data to third parties, how it uses it... The Google Play Store is really trustworthy to me because you know, applications have to get certified by the Play Store... or maybe like a third party that does some other sort of verification on their own"* - P3. Some participants (n=3) mentioned that they would try to **find information about data practices and privacy online** if the app's communications were insufficient.

Key findings: *Participants learned about privacy in FemHealth apps from various sources but often doubted the accuracy of this information or worried about potential biases.*

4.5 Views on Legal Protections and Desired Improvements (RQ4)

Views on current legal protections. While some participants (n=5) believed that there were laws that governed the privacy of digital data related to sexual and reproductive health, the majority (n=11) were unaware of such laws. Although five participants were aware that HIPAA protected medical data in the US, some (n=3) expressed **doubts about whether HIPAA applied to FemHealth apps**: *"I don't even know if HIPAA laws apply to the apps... I think that my personal data is protected by HIPAA, like when ... I go to my own personal doctor... but not with the apps"* - P10.

Almost half of participants (n=6) had **low confidence** in their understanding of the scope and complexities of existing legal protections. For example, P9 was unsure whether the government merely mandated transparency around data practices or also enforced restrictions on specific practices: *"I don't know how much kind of authority they [government] can have over companies, especially if companies are making their own like, privacy agreements and things for consumers to read through... Is currently their only involvement, saying "Hey, you need to legally have some kind of privacy report, privacy statement in place" and that's it? Or does the government say "You know, you can't do XY or Z"?"* - P9. P4 expected companies developing FemHealth apps to consider privacy regulations when choosing where to operate or establish their headquarters—often prioritizing what was most convenient or advantageous for the company rather than for users: *"I think whatever is most convenient for the business and for the government. If Clue's data is stored in Austin, Texas, but Clue's headquarters is in Germany, I think they'd go with whatever is most convenient for them... [but] if the US said, "Move your data here and follow our laws," Texas might end up winning, and all data would be stored and governed by Texas laws."*

Desired improvements in regulatory protections. All participants (n=14) advocated for privacy regulations for FemHealth apps, because they believed that without regulatory pressure developers had little inherent incentive to protect users' privacy: *"I don't think this will come from the goodness of the developers' hearts, but with government pressure... So, pressure from the government to make them be transparent with my data and give me the power to decide how much data I'm willing to share - that would be amazing"* - P13.

Participants suggested ways to strengthen legal privacy protections for FemHealth app users. First, they advocated for existing privacy regulations, such as HIPAA, to **classify FemHealth apps as covered entities** and ensure data protection, even when medical institutions are not directly involved in FemHealth monitoring: *"Make medical privacy laws extend into medically based apps"* - P14. Two participants acknowledged that it was important that these regulations had **bipartisan support** and were **enforced on a federal level** to provide equal protections to all US-based app users.

Second, participants emphasized that **data collection practices of FemHealth apps should be regulated**. For example, they suggested that privacy laws should *mandate* apps to obtain informed consent before collecting data (n=4), be transparent about data practices (n=3), make privacy settings to be enabled by default (n=1), and implement opt-in rather than opt-out mechanisms for data collection (n=1): *"I would love for the lawmakers to require a short, concise fact sheet at the beginning... that everything be opted-in instead of opted-out, that the default always come back to the consumer instead of the default almost always being with the companies"* - P12. P6 highlighted the critical need for regulations specifically addressing data collection from minors using FemHealth apps.

Third, some participants (n=4) wanted privacy laws to **prohibit unauthorized sharing and selling of FemHealth data**: *"I would like to the government and policymakers to protect the consumers of these apps much more than they are clearly doing right now to protect our privacy. ... By not allowing the creators of these apps to share our information and definitely not sell it or share it. Period"* - P10. Similarly, several participants (n=4) expressed a desire to **limit or even prohibit government access to and use of data from FemHealth apps**, such as restricting its admissibility as criminal evidence in court: *"I don't think that data you enter into apps like this should be allowed to be used in a court of law for legal action against you or anybody else"* - P11.

Key findings: *Many participants expressed confusion about legal protections—particularly regarding minors' privacy, the applicability of HIPAA, and the interaction between regional laws governing FemHealth apps. They recognized that government influence over both reproductive rights and privacy regulations created a landscape of competing considerations.*

5 Discussion

5.1 Comparison with Prior Work

Some of the findings of our study differ from or contradict the results of previous studies. For example, a recent vignette study [16] found that participants were not initially prompted about the influence of the 2022 overturn of *Roe v. Wade*, which resulted in a generally low number of responses related to the ruling and confusion as to why law enforcement might seek access to FemHealth data, suggesting a broader lack of awareness of the implications of the overturn on FemHealth app usage and data privacy. In contrast, almost all participants in our study, unprompted, viewed criminalization in the current political climate as a primary risk. This is likely because the awareness of this topic has increased since the Cao et al. [16] study was conducted. Furthermore, some participants in [16] found tracking sexual activity and mental health in FemHealth apps irrelevant and unnecessary, while in our study, participants reported using and valuing this tracking functionality more frequently and, hence, had privacy concerns about it. Lastly, in Cao et al. [16] participants were least concerned about the collection of menstrual data due to its relevance and importance to the functionality of the app, while in our study some participants expressed concerns about the possibility of (mis)inferring abortion from menstrual data (e.g., interpreting a menstrual cycle that was missed or delayed due to stress or health conditions as an abortion). Our finding also highlights that concerns towards FemHealth apps are not limited to users actively seeking or at risk of abortion. Our findings also explain high levels of privacy concerns with FemHealth apps found in quantitative studies (e.g., with pre- and perimenopausal participants in [80]), which initially offered limited qualitative insights. These inconsistencies could be attributed to the methodological differences between [16] and the current study, as the use of researcher-crafted vignettes and a survey-based approach (averaging 14 minutes) may not fully capture the complexity of real-life perceptions and lived experiences when compared to in-depth qualitative interviews.

Another contrasting finding is that, compared to teenagers in [23] whose primary concerns were centered around social risks, such as harassment, doxxing, and conflict with family and friends, legal risks were the most prominent concern among our adult participants, followed by data being sold or used for marketing purposes, psychological harm, and stigma. Teenagers have increased emotional reactivity to social cues which could explain the heightened concerns about social risks as opposed to legal or other types of risks observed in our study with adult population [43].

A novel finding in our study highlights misconceptions about privacy practices in relation to free vs. paid FemHealth apps, which may result in a false sense of security among paid app users. Some of our participants believed that free online apps and services come at an increased cost to privacy over paid versions due to their advertisement-based business model. However, previous work has found few differences between paid and free apps in terms of data sharing with third-party SDKs [44]. Moreover, within FemHealth apps, paid versions may increase data disclosures due to the increased features that paid versions unlock [64, 72].

Our study also sheds light on the information sources used to learn about privacy in FemHealth apps and how trusted these information sources are. Although half of our participants learned about data and privacy practices through the information provided directly by their FemHealth apps, many participants mentioned learning through the media (e.g., news, social media, podcasts) and personal discussions. This was often mentioned in the context of recent political and legal events and subsequent media outbreaks, highlighting their role in shaping perceptions of privacy risk among FemHealth app users.

Similarly to previous findings in [66], participants with lower risk profiles (e.g., living in non-restrictive states or above reproductive age) reporting feeling safer using FemHealth apps. However, restrictions on abortion access are increasing in many states, and FemHealth app data could be weaponized in the future and used retroactively, especially since developers can retain historical data [45]. Such views also overlook broader privacy risks and potential harms to FemHealth app users, extending beyond criminalization to include emotional distress and workplace discrimination, as well as risks posed by FemHealth apps to others (e.g., users' daughters), as mentioned by some participants in our study. In support of the findings of broader privacy research (not focused on Femhealth apps), our participants employed various risk mitigation strategies, including behavioral approaches such as self-censorship [95] and providing inaccurate information [82]. However, withholding data or falsifying information can compromise the accuracy of FemHealth app predictions, thereby preventing users from fully benefiting from these useful and cost-effective tools.

Many of our participants were concerned about the use of their FemHealth app data for marketing and advertising. FemHealth app privacy policy and network traffic analysis has shown how many FemHealth apps share user information with data aggregators and advertising companies [18, 32]. The Flo app has admitted and settled the allegations that they transmitted user data to Meta, Google, and other third parties analytics companies, which could have been used for advertising purposes, although their privacy policy stated at the time that this data was not shared with third-party companies [3, 11, 21, 33, 34]. Although targeted advertising is generally seen by online users as annoying or uncomfortable [63, 92], unsolicited advertising based on sensitive information from FemHealth apps can cause serious psychological harm when targeting is inaccurate [39]. For example, in news articles, people who used FemHealth apps to track pregnancies reported receiving baby-related advertisements and promotional products after experiencing a miscarriage [65, 75] or stillbirth [14]. Our work highlights privacy concerns related to inappropriate disclosures to ad networks, and criminalization threats through disclosure of FemHealth app data to governments and law enforcement. We also found broader concerns about lack of transparency among our participants, in terms of what data is collected in the background or inferred, how data is (or could be) shared, and how data is processed. Such lack of transparency makes it difficult for users to accurately evaluate risks related to app use.

Our study offers rich empirical evidence about FemHealth app users' privacy experiences and concerns, extending beyond the risk of criminalization linked to abortion access to address broader privacy risks and other potential harms. Drawing on these findings, the next sections present recommendations for enhancing FemHealth app user privacy targeted for researchers, FemHealth app designers, developers, platforms and app stores, as well as policymakers.

5.2 Practical Recommendations

We identify the need for more granular and personalized controls, more proactive presentation of reliable privacy information and choices, and better options for data deletion and export in FemHealth apps. In the absence of such controls, participants often avoided the use of FemHealth apps, depriving them of the benefits these apps can otherwise provide.

User controls empowering user autonomy. Prior work has found that transparent privacy interaction design mechanisms correlate with better user experience, increased trust, and more sustained use of beneficial healthcare technologies, like FemHealth apps [8]. FemHealth apps currently lack such mechanisms, as shown in §4.3 and in previous studies [31, 64].

Specifically, some participants experienced (or expected) difficulties in deleting their data from FemHealth Apps, or described emailing developers as the only way they had to request data deletion—a finding confirmed in prior usability inspections of FemHealth apps [64]. This method can be cumbersome, and leaves a paper trail of the request, which could be leveraged against users as evidence in a criminal investigation—a problem less common for non-FemHealth context, where app usage data is less likely to be incriminating. Consequently, we highlight an urgent need for developing easy to find and use app features for data deletion and export from FemHealth apps, and guarantees that no backup copy or paper trail is retained after data deletion. Users may also be offered an opt in to automatic periodic data deletion or choose the duration of data storage, since our participants acknowledged that their historic period-tracking data would lose value over time, and often only the most recent observations were informative or useful.

We also identify a need for more discreet notifications and app locks (additional authentication steps for unlocking FemHealth apps), to avoid unintended information disclosures to those within close proximity of the user. Additionally, privacy settings should allow users to manage what inferences FemHealth apps are allowed to make about them, and who gets access to sensitive user data. Explicit and revocable user consent should be required before sharing or using FemHealth app data for marketing and advertising. Priority should be given to privacy-by-default settings and opt-in rather than opt-out mechanisms. Finally, FemHealth apps may choose identity models that rely on pseudonyms (and explicitly discourage users to use their real names) to avoid the collection of PII, and reduce the risks of de-identification; the use of real names in FemHealth apps also has no obvious benefits compared to social media, for example, where real names can help find and connect with friends. While these recommendations could protect privacy in other genres of apps too, they are especially important to adhere to in FemHealth app context, due to particular sensitivity of the data these apps collect and severity of risks they raise (see §4.2).

Future work should engage FemHealth users in co-designing novel privacy controls that are grounded in users' lived experiences, clearly communicate app risks to users, empower users to find the right balance between benefits and risks, and to control their data.

Proactive dynamic risk-based privacy prompts. Our findings suggest that onboarding (when users install and set up the account for the app) is an important moment to engage users to think about their privacy by providing them with information and consent mechanisms, as well as privacy choices. Although onboarding may be a good moment to start engaging with users in relation to their privacy, the dynamic changes in privacy risks posed by FemHealth apps [66], e.g., due to changes not only in the regulatory privacy protections, but also in the reproductive rights, require regular updating of users' knowledge about the data practices of the apps and related risks. For example, if a user moves to a state with greater restrictions on reproductive rights, they will be subject to a greater risk than when they initially created their app account, thus, they may need to reconsider their privacy choices and configurations of settings. Yet, we found that participants rarely revisited their privacy choices after onboarding. FemHealth apps should consider dynamic risk safeguards [74] that promptly respond to changes in the regulatory landscape or users' location, and inform users (e.g., via in-app or email notifications) and those who consider installing FemHealth apps (e.g., via disclosures in app stores) about privacy risks that such changes bring. Similarly to how Tinder and Grindr alerts its LGBTQ users when they travel to a country that criminalizes their sexuality [1, 74], FemHealth apps could use risk metrics to inform the timing and guidance of proactive privacy prompts to support users in reflecting on their privacy choices, and how these choices align with their risk profile. However, we acknowledge that location-based prompts specifically may pose additional privacy risks, as they require the collection of location data our participants were worried about. Thus, apps should exercise caution when designing contextual notifications, and avoid amplifying or imposing new privacy risks to users. Such risk mitigation could include local processing of location data, as opposed to server-side processing. FemHealth apps can periodically invite users to perform a privacy checkup or revisit their settings after a significant event that may change the risk profile (e.g., after a user has entered information about miscarriage, abortion, or pregnancy, or when it was inferred). FemHealth apps may also ask users to confirm the accuracy of inferences to avoid potential misattribution.

Improved transparency. Beyond usable privacy mechanisms, our work highlights the need for greater transparency around data flows, allowing users to understand whether their data is shared with advertisers or law enforcement, which is of particular concern for FemHealth app users due to their concerns with criminalization and unethical or emotionally harmful ads related to reproductive health, as discussed in §5.1. Similarly, FemHealth apps should disclose not only what health data they collect, but also what they can *infer* from it, including potential pregnancies, abortions, miscarriages, health conditions or sexually transmitted diseases. Accuracy of such inferences is especially important in the FemHealth context, as they can lead to wrongful criminalization, discrimination, traumatizing, and stigmatization. Some participants expressed skepticism about the trustworthiness of information presented by a FemHealth app, whether within the app itself or in their privacy policies, suspecting that financial interests could take precedence over honest privacy disclosures. Some participants also did not trust government sources, given past breaches of trust and the potential for political bias in the sates with restrictions on reproductive rights. Thus, FemHealth apps need to build trust with users by exerting efforts in providing extensive privacy protections and controls, and presenting evidence from third-party privacy and security assessments and audits. However, we draw attention to the risk of "privacy-washing", where assurances disseminated through unofficial channels (e.g., ads) mislead users while obscuring potentially risky privacy practices [17]. Independent researchers and organizations, like Consumer Reports or Electronic Frontier Foundation (EFF), could assess and publish reports about data practices and privacy in FemHealth apps, and expose violations or inaccuracies in privacy disclosures. App stores can display the privacy rating of apps (e.g., similar to Privacy Badger [29]).

Open-source FemHealth apps. No participant mentioned offline or free and open-source (FOSS) period trackers that ran entirely on the user's device and did not collect any data [26]. In principle, these apps would address privacy concerns our participants raised by offering users autonomous control over their data, untraceability, and transparency around how features are implemented by virtue of the source code being openly available. However, user studies of open-source apps are currently scarce. Enhancing scholarly understanding of open-source FemHealth apps (e.g., user perceptions of safety, addressing the risk of users losing or breaking a device) can drive community-led innovation in FemHealth apps, and inform well-rounded privacy guidance for users.

Although prior work [16, 48] made practical recommendations about transparency (e.g., privacy summaries, visual aids) and user control (e.g., selective agreement), we expand with further actionable FemHealth-specific measures from our data such as user controls for periodic data deletion, discreet notifications and app locks, correction of inferences made by FemHealth apps, contextual privacy alerts, and use of open-source code for FemHealth apps.

5.3 Policy Implications and Recommendations

Some participants recognized HIPAA as the primary law governing the security and privacy of mobile health app data collected and processed by healthcare providers and related entities. However, participants were uncertain whether HIPAA applied to FemHealth apps, though they believed it should. In reality, HIPAA does not cover mobile health apps not provided by a covered entity, such as a healthcare provider, health insurance plan, or clearinghouse. Thus, similarly to many other apps collecting health data [40, 62, 89], FemHealth apps are typically not subject to HIPAA requirements. Some participants also expected data protection laws like HIPAA to prohibit sharing user health data with law enforcement. However, recent work has shown that many FemHealth apps are required to share data with authorities if subpoenaed [64]. It raises concerns about the interplay between data protection and anti-abortion laws in the US, and the possibility of weaponizing FemHealth apps and consumer data to criminalize those seeking, providing, and supporting abortion care. We recommend enacting laws that prevent sexual and reproductive health data from being used to prosecute FemHealth app users, as proposed by our participants in §4.5. For instance, California passed the Assembly Bill (AB) 254 and AB 1697, extending privacy protections to reproductive and sexual health information to apps' and websites' users [90]. However, there remains a need for *federal* legislation to protect digital data that crosses state lines, ensuring that all FemHealth app users receive equal protection regardless of where they reside in the US.

Overall, our participants had low confidence in understanding HIPAA protections, and often misunderstood them, which could in of itself create risks where users expect a higher degree of privacy protection through regulation than is required in practice. Additionally, although the FTC Act [19] and the Health Breach Notification Rule (HBNR) [20] regulate deceptive data practices and require data breach notifications in FemHealth apps, none of our participants were aware of them. This warrants the need for raising public awareness about privacy rights and regulatory protections, for example, through news stories, user-friendly infographics and articles distributed by trusted organizations that advocate for user privacy (e.g., EFF, IAPP, EPIC, etc.), and explicit acknowledgment of different regulations that the app is intended to comply with in privacy policies and other user-facing privacy disclosures.

Additionally, app marketplaces should require FemHealth app developers to disclose if they share or intend to share all, or at least sensitive sexual and reproductive health data (or any inferences), with law enforcement or third-party processors (including advertisement networks). For example, currently, Google Play does not require developers to disclose when data is shared with "a service provider to process it [data] on the developer's behalf" or when data is "transferred for specific legal purposes, such as in response to a government request" [41]. This is particularly concerning in the context of FemHealth apps, as the app developer could be based in California with stronger legal protections for privacy and reproductive rights, but the data can be stored in Texas, where such protections are weaker. Moreover, we found that some participants incorrectly believed that marketplaces verified (or 'certified') data safety information disclosed by app developers, which resulted in higher trust in these disclosures. Furthermore, several participants trusted FemHealth apps developed in the EU due to GDPR protections, but this is a misconception. Although GDPR provides some protections, it has numerous exceptions that can undermine user privacy [69]. Also, even within the limited scope of current regulations, including GDPR, non-compliant practices and poor adherence to laws by developers are still observed [69]. Moreover, recent research has shown that EU-based FemHealth apps can still transfer user data to US-based processors or other regions with weaker regulations [64]. Thus, app store disclosure exemptions, user misconceptions, and inaccuracies in app disclosures [52–54, 96] have serious privacy implications for users by making it difficult for them to assess risks and make informed privacy decisions [64]. Thus, we recommend that app stores mandate and, importantly, *verify* full privacy disclosures to promote realistic expectations and build user trust in FemHealth apps.

To summarize, our work not only provides additional empirical evidence that supports prior recommendations, e.g., to increase transparency about law enforcement data access and address users' misconceptions about legal protections [e.g., as in 16], but also emphasizes the need for extending the existing legal protections (e.g., HIPAA) to FemHealth apps, advocating for federal safeguards, and highlights unique tensions between data protection and abortion laws unique to the FemHealth app genre.

6 Conclusion

FemHealth apps offer promising opportunities to enhance personal health management, narrow the gender health gap, and promote greater health equity and affordability, but they also pose significant privacy and security risks. Our interviews with 14 FemHealth app users in the US highlight the complex and often conflicting rols these apps play in users' lives. Participants viewed FemHealth app data as highly sensitive and expressed stronger privacy concerns about these apps than about non-health apps, citing risks of criminalization, location tracking, and potential psychological harm or stigmatization resulting from data breaches. To mitigate these risks, participants proposed a range of strategies—from user-facing measures such as clearer privacy disclosures and enhanced privacy controls to back-end protections that do not rely on active user engagement. Yet, our findings revealed wide variation in users' trust toward both governmental and app-provided privacy information, alongside broad uncertainty about existing regulatory safeguards. These insights underscore the need for comprehensive interventions, including improved design to increase transparency and user control, stronger technical protections, and expanded regulatory frameworks tailored to the unique sensitivities of FemHealth app data. Future research should explore how design, regulation, and user education can support informed and autonomous engagement with FemHealth apps—maximizing their benefits while minimizing privacy risks and structural vulnerabilities.

Acknowledgments

We thank the reviewers of SOUPS and PETS conferences for valuable feedback that helped us improve the manuscript. We thank all participants for generously sharing their time and experiences. This research was supported by the U.S. National Science Foundation (award CNS-2055772).

References

[1] Traveler Alert – Tinder. https://www.help.tinder.com/hc/en-us/articles/30627581230605-Traveler-Alert.

[2] Dobbs v. Jackson Women's Health Organization, 2022. 597 US.

[3] Flo Health settles class action over personal health data sharing, 2025. URL https://iclg.com/news/22904-flo-health-settles-class-action-over-personal-health-data-sharing#:~:text=Flo%20Health%2C%20creator%20of%20the,among%20other%20third%20parties%2C%20in.

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

[5] Teresa Almeida, Laura Shipp, Maryam Mehrnezhad, and Ehsan Toreini. Bodies Like Yours: Enquiring Data Privacy in FemTech. In Adjunct Proceedings of the 2022 Nordic Human-Computer Interaction Conference (NordiCHI '22), pages 1–5, October 2022.

[6] Marco Altini and Daniel Plews. What is behind changes in resting heart rate and heart rate variability? a large-scale analysis of longitudinal measurements acquired in free-living. Sensors, 21(23):7932, 2021.

[7] Katrin Amelang. (Not) safe to use: insecurities in everyday data practices with period-tracking apps. In New Perspectives in Critical Data Studies: The Ambivalences of Data Power, pages 297–321. Springer, 2022.

[8] Oshrat Ayalon, Dana Turjeman, and Elissa M Redmiles. Exploring privacy and incentives considerations in adoption of COVID-19 contact tracing apps. In 32nd USENIX Security Symposium, pages 517–534, 2023.

[9] Loraine J Bacchus, Kate Reiss, Kathryn Church, Manuela Colombini, Erin Pearson, Ruchira Naved, Chris Smith, Kathryn Andersen, and Caroline Free. Using digital technology for sexual and reproductive health: are programs adequately considering risk? Global Health: Science and Practice, 7(4):507–514, 2019.

[10] Naveen Basavaraj, Uttara M Ananthakrishnan, and Catherine E Tucker. The chilling effect of Dobbs: A study of mobile health apps usage. SSRN 4924919, 2024.

[11] Karissa Bell. Period tracking app says it will stop sharing health data with Facebook. https://mashable.com/article/flo-period-tracking-app-will-stop-sharing-data-with-facebook/, 2019.

[12] José Patrício Bispo Júnior. Social desirability bias in qualitative health research. Revista de saude publica, 56:101, 2022.

[13] Anna Broad, Rina Biswakarma, and Joyce C Harper. A survey of women's experiences of using period tracker applications: Attitudes, ovulation prediction and how the accuracy of the app in predicting period start dates affects their feelings and behaviours. Women's health, 18:17455057221095246, 2022.

[14] Gillian Brockell. Dear Tech Companies, I don't want to see pregnancy ads after my child was stillborn". https://www.washingtonpost.com/lifestyle/2018/12/12/dear-techcompanies-i-dont-want-see-pregnancy-ads-after-my-child-was-stillborn/, 2018.

[15] Kelly Caine. Local standards for sample size at chi. In Proceedings of the 2016 CHI conference on human factors in computing systems, pages 981–992, 2016.

[16] Jiaxun Cao, Hiba Laabadli, Chase H Mathis, Rebecca D Stern, and Pardis Emami-Naeini. "I deleted it after the overturn of Roe v. Wade": Understanding women's privacy concerns toward period-tracking apps in the post Roe v. Wade era. In Proceedings of the CHI Conference on Human Factors in Computing Systems, pages 1–22, 2024.

[17] Angela M. Cirucci. Oversharing the super safe stuff: "privacy-washing" in apple iphone and google pixel commercials. First Monday, 29(5), May 2024. doi: 10.5210/fm.v29i5.13321. URL https://firstmonday.org/ojs/index.php/fm/article/view/13321.

[18] Andreas Claesson and Tor E Bjørstad. Technical report:'out of control'—a review of data sharing by popular mobile apps. Report for the Norwegian Consumer Council, 14, 2020.

[19] Federal Trade Commission. Federal Trade Commission Act, . URL https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act.

[20] Federal Trade Commission. Health Breach Notification Rule, . URL https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule.

[21] Federal Trade Commission et al. Developer of popular women's fertility-tracking app settles ftc allegations that it misled consumers about the disclosure of their health data. Press Release, 2021.

[22] Joseph Cox. Data broker is selling location data of people who visit abortion clinics. Vice News, 3, 2022.

[23] Umama Dewan, Cora Sula, and Nora Mcdonald. Teen reproductive health information seeking and sharing post-roe. In Proceedings of the CHI Conference on Human Factors in Computing Systems, pages 1–12, 2024.

[24] Zikan Dong, Liu Wang, Hao Xie, Guoai Xu, and Haoyu Wang. 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), pages 1–6, New York, NY, USA, October 2022. ACM.

[25] J Dreaper. Women warned about booming market in period tracker apps. BBC News, 2016.

[26] Drip.app. Drip. period and fertility app. URL https://bloodyhealth.gitlab.io/.

[27] Sarah Earle, Hannah R Marston, Robin Hadley, and Duncan Banks. Use of menstruation and fertility app trackers: a scoping review of the evidence. BMJ sexual & reproductive health, 47(2):90–101, 2021.

[28] Sarah Earle, Hannah R Marston, Robin Hadley, and Duncan Banks. Use of menstruation and fertility app trackers: A scoping review of the evidence. BMJ Sexual & Reproductive Health, 47(2):90–101, Apr. 2021.

[29] Electronic Frontier Foundation. Privacy Badger. https://privacybadger.org/, 2025.

[30] Kweilin Ellingrud, Lucy Pérez, Anouk Petersen, and Valentina Sartori. Closing the women's health gap: a $1 trillion opportunity to improve lives and economies. McKinsey Health Institute, 11:2024, 2024. URL https://www.mckinsey.com/mhi/our-insights/closing-the-womens-health-gap-a-1-trillion-dollar-opportunity-to-improve-lives-and-economies.

[31] Daniel A Epstein, Nicole B Lee, Jennifer H Kang, Elena Agapie, Jessica Schroeder, Laura R Pina, James Fogarty, Julie A Kientz, and Sean Munson. Examining menstrual tracking to inform the design of personal informatics tools. In Proceedings of the CHI conference on human factors in computing systems, pages 6876–6888, 2017.

[32] Jacob Erickson, Jewel Y. Yuzon, and Tamara Bonaci. What You Do Not Expect When You Are Expecting: Privacy Analysis of Femtech. IEEE Transactions on Technology and Society, 3(2):121–131, Jun. 2022.

[33] Inc. Flo Health. Flo statement on data privacy. Flo.Health - #1 mobile product for women's health. https://flo.health/users-privacy-and-data-security, 2019.

[34] Inc. Flo Health. Flo privacy policy. Flo.Health - #1 mobile product for women's health. https://flo.health/privacypolicy, 2020.

[35] Leah R. Fowler, Charlotte Gillard, and Stephanie R. Morain. Readability and Accessibility of Terms of Service and Privacy Policies for Menstruation-Tracking Smartphone Applications. Health Promotion Practice, 21(5):679–683, September 2020.

[36] Sarah Fox, Noura Howell, Richmond Wong, and Franchesca Spektor. Vivewell: Speculating Near-Future Menstrual Tracking through Current Data Practices. In Proceedings of the on Designing Interactive Systems Conference, pages 541–552, June 2019.

[37] Jill J Francis, Marie Johnston, Clare Robertson, Liz Glidewell, Vikki Entwistle, Martin P Eccles, and Jeremy M Grimshaw. What is an adequate sample size? operationalising data saturation for theory-based interview studies. Psychology and health, 25(10):1229–1245, 2010.

[38] Katie Gambier-Ross, David J McLernon, and Heather M Morgan. A mixed methods exploratory study of women's relationships with and uses of fertility tracking apps. Digital Health, 4:2055207618785077, 2018.

[39] Michele Estrin Gilman. Periods for profit and the rise of menstrual surveillance. Colum. J. Gender & L., 41:100, 2021.

[40] Tasha Glenn and Scott Monteith. Privacy in the digital world: medical and health data outside of hipaa protections. Current psychiatry reports, 16(11):494, 2014.

[41] Google. Understand app privacy security practices with Google Play's Data safety section - Computer - Google Play Help. https://support.google.com/googleplay/answer/11416267. Accessed on 13.02.2025.

[42] Greg Guest, Arwen Bunce, and Laura Johnson. How many interviews are enough? an experiment with data saturation and variability. Field methods, 18(1):59–82, 2006.

[43] Simone PW Haller, Kathrin Cohen Kadosh, Gaia Scerif, and Jennifer YF Lau. Social anxiety disorder in adolescence: How developmental cognitive neuroscience findings may shape understanding and interventions for psychopathology. Developmental cognitive neuroscience, 13:11–20, 2015.

[44] Catherine Han, Irwin Reyes, Álvaro Feal, Joel Reardon, Primal Wijesekera, Narseo Vallina-Rodriguez, Amit Elazari, Kenneth A Bamberger, and Serge Egelman. The price is (not) right: Comparing privacy in free and paid apps. Proceedings on Privacy Enhancing Technologies, 2020.

[45] Kashmir Hill. Deleting your period tracker won't protect you. https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html, 2023.

[46] Bryndl Hohmann-Marriott. Periods as powerful data: User understandings of menstrual app data and information. New Media & Society, 25(11):3028–3046, 2021.

[47] Minji Hong, Vasuki Rajaguru, KyungYi Kim, Suk-Yong Jang, and Sang Gyu Lee. Menstrual cycle management and period tracker app use in millennial and generation z individuals: Mixed methods study. Journal of Medical Internet Research,

26:e53146, 2024.

[48] Anna Ida Hudig and Jatinder Singh. Intimate data sharing: Enhancing transparency and control in fertility tracking. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, pages 1–24, 2025.

[49] Sarah J Iribarren, Kenrick Cato, Louise Falzon, and Patricia W Stone. What is the economic evidence for mhealth? a systematic review of economic evaluations of mhealth solutions. PloS one, 12(2):e0170581, 2017.

[50] Reema A Karasneh, Sayer I Al-Azzam, Karem H Alzoubi, Suhaib M Muflih, and Sahar S Hawamdeh. Smartphone applications for period tracking: rating and behavioral change among women users. Obstetrics and Gynecology International, 2020(1):2192387, 2020.

[51] Erin Kenneally and David Dittrich. The Menlo report: Ethical principles guiding information and communication technology research. Available at SSRN 2445102, 2012.

[52] Rishabh Khandelwal, Asmit Nayak, Paul Chung, Kassem Fawaz, Antonio Bianchi, et al. Unpacking privacy labels: A measurement and developer perspective on Google's data safety section. In 33rd USENIX Security Symposium, pages 2831–2848, 2024.

[53] Simon Koch, Malte Wessels, Benjamin Altpeter, Madita Olvermann, and Martin Johns. Keeping privacy labels honest. Proceedings on Privacy Enhancing Technologies, 2022.

[54] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. Goodbye tracking? impact of iOS app tracking transparency and privacy labels. In Proceedings of the ACM Conf. on Fairness, Accountability, and Transparency, pages 508–520, 2022.

[55] Katie Krumbholz, Alice Militaru, and Kyle J Morgan. Tracking the trackers: 'menstruapp' privacy policies following the dobbs decision. Journal of Women, Politics & Policy, 45(1):167–189, 2024.

[56] Robert S Laufer and Maxine Wolfe. Privacy as a concept and a social issue: A multidimensional developmental theory. Journal of Social Issues, 33(3):22–42, 1977.

[57] Natasa Lazarevic, Marie Lecoq, Céline Bœhm, and Corinne Caillaud. 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):1012, January 2023.

[58] Natasa Lazarevic, Carol Pizzuti, Gillian Rosic, Céline Bœhm, Kathryn Williams, and Corinne Caillaud. A mixed-methods study exploring women's perceptions and recommendations for a pregnancy app with monitoring tools. NPJ Digital Medicine, 6(1):50, 2023.

[59] Johanna Levy and Nuria Romo-Avilés. 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):1213, December 2019.

[60] Karen Levy. Intimate Surveillance. Idaho Law Review, 51(3), Sep. 2015.

[61] Yanzi Lin, Jaideep Juneja, Eleanor Birrell, and Lorrie Faith Cranor. Data safety vs. app privacy: Comparing the usability of android and ios privacy labels. Proceedings on Privacy Enhancing Technologies, 2024(2), 2024.

[62] David D Luxton, Robert A Kayl, and Matthew C Mishkind. mhealth data security: The need for hipaa-compliant standardization. Telemedicine and e-Health, 18(4): 284–288, 2012.

[63] Miguel Malheiros, Charlene Jennett, Snehalee Patel, Sacha Brostoff, and Martina Angela Sasse. Too close for comfort: A study of the effectiveness and acceptability of rich-media personalized advertising. In Proceedings of the SIGCHI conference on human factors in computing systems, pages 579–588, 2012.

[64] Lisa Mekioussa Malki, Ina Kaleva, Dilisha Patel, Mark Warner, and Ruba Abu-Salma. Exploring privacy practices of female mhealth apps in a post-roe world. In Proceedings of the CHI Conference on Human Factors in Computing Systems, pages 1–24, 2024.

[65] Olga Massov. Pregnancy apps don't know how to handle miscarriages. https://mashable.com/article/miscarriage-stillbirth-pregnancy-apps/, 2018.

[66] Nora Mcdonald and Nazanin Andalibi. "I Did Watch 'The Handmaid's Tale'": Threat Modeling Privacy Post-roe in the United States. ACM Transactions on Computer-Human Interaction, 30(4):1–34, 2023.

[67] Maryam Mehrnezhad and Teresa Almeida. Caring for Intimate Data in Fertility Technologies. In Proceedings of the CHI Conference on Human Factors in Computing Systems, pages 1–11, May 2021.

[68] Maryam Mehrnezhad and Teresa Almeida. "My sex-related data is more sensitive than my financial data and I want the same level of security and privacy": User Risk Perceptions and Protective Actions in Female-oriented Technologies. In Proceedings of the European Symposium on Usable Security, pages 1–14, 2023.

[69] Maryam Mehrnezhad, Thyla Van Der Merwe, and Michael Catt. Mind the femtech gap: regulation failings and exploitative systems. Frontiers in the Internet of Things, 3:1296599, 2024.

[70] Diana P. Moniz, Maryam Mehrnezhad, and Teresa Almeida. Intimate data: Exploring perceptions of privacy and privacy-seeking behaviors through the story completion method. In Human-Computer Interaction – INTERACT 2023, pages 533–543, 2023.

[71] National Women's Law Center. States Take Action to Stop Discrimination Based on Reproductive Health Care Decisions. https://nwlc.org/resource/states-take-action-to-stop-discrimination-based-on-reproductive-health-care-decisions/, 2024.

[72] Nidhi Nellore, Tania Mishra, and Michael Zimmer. Unveiling user perspectives: Exploring themes in femtech mobile app reviews for enhanced usability and privacy. Proceedings of the ACM on Human-Computer Interaction, 8(MHCI): 1–21, 2024.

[73] Sophie L Nelson. The post-dobbs reality: Privacy expectations for period-tracking apps in criminal abortion prosecutions. Pepp. L. Rev., 51:783, 2024.

[74] Catherine RK O'Brien, Nuur Alifah Roslan, Steven J Murdoch, Ruba Abu-Salma, Douglas Zytko, and Mark Warner. Online dating platform safeguards and self-protection: How dating platforms characterise, respond to, and safeguard against harms. In Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems, pages 1–8, 2025.

[75] Amy Pittman. The Internet thinks I'm still pregnant. https://www.nytimes.com/2016/09/04/fashion/modern-love-pregnancy-miscarriage-app-technology.html, 2016.

[76] Eugenia Politou, Efthimios Alepis, and Constantinos Patsakis. Forgetting personal data and revoking consent under the gdpr: Challenges and proposed solutions. Journal of cybersecurity, 4(1):tyy001, 2018.

[77] Anya ER Prince. Reproductive health surveillance. BCL Rev., 64:1077, 2023.

[78] Francesco Rampazzo, Alyce Raybould, Pietro Rampazzo, Ross Barker, and Douglas Leasure. "UPDATE: I'm pregnant!": Inferring global downloads and reasons for using menstrual tracking apps. Digital Health, 10:20552076241298315, 2024.

[79] Kellen Safreed. Data protection law: The gdpr, ccpa, and us federal regulation. REV. BANKING & FIN. L., 39:115–123, 2019.

[80] Gabrielle M Salvatore, Iris Bercovitz, and Danielle Arigo. Women's comfort with mobile applications for menstrual cycle self-monitoring following the overturning of roe v. wade. Mhealth, 10:1, 2023.

[81] Margarete Sandelowski. Sample size in qualitative research. Research in nursing & health, 18(2):179–183, 1995.

[82] Shruti Sannon, Natalya N Bazarova, and Dan Cosley. Privacy lies: Understanding how, when, and why people lie to protect their privacy in multiple online contexts. In Proceedings of the CHI conference on human factors in computing systems, pages 1–13, 2018.

[83] Allysan Scatterday. 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):636, 2022.

[84] Laura Shipp and Jorge Blasco. How private is your period?: A systematic analysis of menstrual app privacy policies. Proceedings on Privacy Enhancing Technologies, 2020(4):491–510, October 2020.

[85] Qiurong Song, Rie Helene Hernandez, Yubo Kou, and Xinning Gui. "Our Users' Privacy is Paramount to Us": A Discourse Analysis of How Period and Fertility Tracking App Companies Address the Roe v Wade Overturn. In Proceedings of the CHI Conference on Human Factors in Computing Systems, pages 1–21, 2024.

[86] Qiurong Song, Renkai Ma, Yubo Kou, and Xinning Gui. Collective Privacy Sensemaking on Social Media about Period and Fertility Tracking post Roe v. Wade. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW1): 1–35, 2024.

[87] Qiurong Song, Yanlai Wu, Rie Helene Hernandez, Yao Li, Yubo Kou, and Xinning Gui. Understanding users' perception of personally identifiable information. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, pages 1–24, 2025.

[88] Anne Stopper and Jen Caltrider. See no evil: Loopholes in Google's Data Safety labels keep companies in the clear and consumers in the dark. URL https://foundation.mozilla.org/en/campaigns/googles-data-safety-labels/.

[89] Kim Theodos and Scott Sittig. Health information privacy laws in the digital age: Hipaa doesn't apply. Perspectives in health information management, 18 (Winter):1l, 2020.

[90] Elizabeth Tobin-Tyler and Eli Adashi. Protecting sexual and reproductive health privacy post-dobbs. JAMA Internal Medicine, 2024.

[91] Anupriya Tuli, Surbhi Singh, Rikita Narula, Neha Kumar, and Pushpendra Singh. Rethinking Menstrual Trackers Towards Period-Positive Ecologies. In Proceedings of the CHI Conference on Human Factors in Computing Systems, pages 1–20, April 2022.

[92] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. Smart, useful, scary, creepy: perceptions of online behavioral advertising. In Proceedings of the Eighth Symposium on Usable Privacy and Security, pages 1–15, 2012.

[93] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (un) informed consent: Studying gdpr consent notices in the field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pages 973–990, 2019.

[94] Konstantina Vasileiou, Julie Barnett, Susan Thorpe, and Terry Young. Characterising and justifying sample size sufficiency in interview-based studies: systematic

analysis of qualitative health research over a 15-year period. BMC medical research methodology, 18(1):148, 2018.

[95] Mark Warner and Victoria Wang. Self-censorship in social networking sites (snss)–privacy concerns, privacy awareness, perceived vulnerability and information management. Journal of Information, Communication and Ethics in Society, 17(4):375–394, 2019.

[96] Yue Xiao, Zhengyi Li, Yue Qin, Xiaolong Bai, Jiale Guan, Xiaojing Liao, and Luyi Xing. Lalaine: Measuring and characterizing non-compliance of apple privacy labels. In 32nd USENIX Security Symposium, pages 1091–1108, 2023.

A Study Materials

A.1 Screening Survey

1. Have you used a mobile app (or apps) to track your period, fertility, pregnancy, or other areas of your sexual and reproductive health? 1) I currently use one or more apps for this purpose, 2) I used one or more apps for this purpose in the past, but I do not use any currently, 3) I have never used an app for this purpose

2. What operating system do you use on your main mobile device? 1) Android, 2) Apple (iOS), 3) Other (please specify)

3. Please select the mobile app (or apps) you use (or used) from the list below. 1) Apple Health, 2) Google Fit, Samsung Health or other built-in Android health app, 3) Flo Ovulation and Period Tracker, 4) Clue Period Tracker and Calendar, 5) Natural Cycles, 6) Glow Period Tracker, 7) Maya Period Tracker, 8) Pregnancy+, 9) Glow Nurture Pregnancy Tracker, 10) Ovia Pregnancy Tracker, 11) BabyCenter Pregnancy Tracker, 12) Other, please specify. If possible, please provide a link to the app's webpage in the Apple Store or Google Play Store, so that we can identify it easily.

4. Please indicate the *one app* you use/used the most. 1) Apple Health, 2) Google Fit, Samsung Health or other built-in Android health app, 3) Flo Ovulation and Period Tracker, 4) Clue Period Tracker and Calendar, 5) Natural Cycles, 6) Glow Period Tracker, 7) Maya Period Tracker, 8) Pregnancy+, 9) Glow Nurture Pregnancy Tracker, 10) Ovia Pregnancy Tracker, 11) BabyCenter Pregnancy Tracker, 12) Other, please specify. If possible, please provide a link to the app's webpage in the Apple Store or Google Play Store, so that we can identify it easily.

5. What term do you believe would be most appropriate to describe apps designed to track periods, pregnancy, fertility, and other areas of sexual and reproductive health, based on your personal preference?

6. Next, we will ask several questions related to diversity and inclusion. You will not be excluded from the study on the basis of your answer to these questions. Please select the group that best describes you from the options below. 1) White or Caucasian, 2) Black or African American, 3) Asian or Asian American, 4) Native Hawaiian or Other Pacific Islander, 5) American Indian or Alaska Native, 6) Arab or North African, 7) Mixed or multiple groups (please specify), 8) Prefer to self-describe, 9) Prefer not to say.

7. What is your gender? 1) Woman, 2) Man (2), 3) Non-binary or prefer to self-describe, 4) Prefer not to say.

8. What is your highest level of education? 1) Less than high school, 2) High school/GED or equivalent, 3) Some college or university but no degree, 4) Associate degree, 5) Bachelor's degree or equivalent, 6) Master's degree or equivalent, 7) Doctoral or professional degree (PhD, JD, MD, 8) Other, please specify, 9) Prefer not to say.

9. How would you describe your current employment status? 1) Unemployed, 2) Employed full-time, 3) Employed part-time or casually, 4) Self-employed, 5) Student, 6) Retired, 7) Other (please specify), 8) Prefer not to say.

10. Do you have education or work experience in any of the information technology fields (such as Computer Science, Software Engineering, App Development, etc.)? 1) Yes, 2) No.

11. Do you use any of the following privacy-protecting tools, software or features on a regular basis? 1) Virtual Private Networks (VPNs), 2) End-to-end encryption (e.g., encrypted emails), 3) Private browsing (e.g., Incognito mode), 4) Tor Browser, 5) DuckDuckGo search engine, 6) Password managers, 7) Other (please specify), 8) None of the above.

12. Please indicate on the slider below how concerned you are about how the mobile app (or apps) you have used handles (or handle) your sexual and reproductive health data, where 1 is the least concerned, and 10 is the most concerned.

[For Past users:]

13. When was the last time you used a mobile app (or apps) to track your period, fertility, pregnancy, or other areas of your sexual and reproductive health? 1) Less than 1 month ago, 2) 1–3 months ago, 3) 3–6 months ago, 4) 6 months to a year ago, 5) Over a year ago, 6) Prefer not to say.

14. Please select the app features you made use of while using the app from the list below. 1) Cycle tracking, 2) Period predictions, 3) Fertility or ovulation predictions, 4) Menopause tracking, 5) Sexual activity tracking, 6) Mood and mental health tracking, 7) Physical symptom tracking, 8) Pregnancy tracking, 9) Birth control management, 10) In-app forums or communities, 11) Push-notifications and reminders, 12) Other, please specify, 13) None of the above, 14) Prefer not to say.

15. Why did you stop using the app(s)? Please select all that apply. 1) I did not need the app(s) anymore, 2) I found the app(s) difficult to use, 3) I had technical issues with the app(s) (e.g., running out of storage, app crashes), 4) I had privacy-related concerns, 5) Other (please specify).

[For Current users:]

16. How often do you use a mobile app (or apps) to track your period, fertility, pregnancy, or other areas of your sexual and reproductive health? 1) Daily, 2) Weekly, 3) Monthly, 4) Other (please specify), 5) Prefer not to say.

17. Please select the app features you regularly make use of from the list below. 1) Cycle tracking, 2) Period predictions, 3) Fertility or ovulation predictions, 4) Menopause tracking, 5) Sexual activity tracking, 6) Mood and mental health tracking, 7) Physical symptom tracking, 8) Pregnancy tracking, 9) Birth control management, 10) In-app forums or communities, 11) Push-notifications and reminders, 12) Other, please specify, 13) None of the above, 14) Prefer not to say.

[For All users:]

18. Please briefly describe why you are interested in participating in this study.

19. Please provide your current time zone. If you are invited for an interview, this will help us schedule it at a time that is convenient for you.

A.2 Interview Script

Today I will be asking you questions about your views on and personal experiences with mobile apps that track period, fertility, pregnancy, or other areas of sexual and reproductive health, as well as your understanding of how your data is handled by these apps. App industry often refers to this category of apps as Female Health apps. Do you have a preference if throughout the interview I am referring to them as "period and fertility tracking apps" or "Female Health apps"? [Refer to them according to participants' preference throughout.][2]

A.2.1 General Views and Experiences.

We will start by asking questions about your views on and personal experiences with [APP] in particular, the app you said you use (or had used in the past) the most. Female mobile health apps are specifically designed to support various aspects of female sexual and reproductive health. These apps offer information, tools, and features to help users manage their health, track menstrual cycles and sexual activity, monitor fertility, pregnancy, and menopause, manage the contraceptives, access personalized health advice, and improve healthcare access and affordability.

1) How long have you used [APP]?
2) What are the main benefits of using [APP] that you noticed?
3) What are the main drawbacks (if any) of using [APP] that you noticed? *[Do not prompt participants to talk about privacy concerns here.]*

If participants use generic fitness or m-health apps (rather than specialized FemHealth apps), focus their attention on FemHealth related use cases and features only, so they don't get side-tracked with discussions about activity, sleep, diet, etc.

It sounds like you've been using [APP] for both [use cases]. For the scope of our conversation today, we will focus only on your use of this app for tracking periods, fertility, pregnancy, sexual or reproductive health. OK?

A.2.2 Data Flows: Beliefs and Feelings about Data Flows.

1) What types of data do you think [APP] collects? *[Probe: What health-related data do you think* [APP] *collects?]*

a) What data do you provide by yourself when using [APP]?

b) What data, if any, does [APP] collect automatically, by itself? [*Probe: Can you make a guess*?]

c) Do you have any negative feelings about collection of any of the data types you mentioned? If so, what data and why?

d) In contrast, what data types do you feel comfortable with their collection, and why?

2) What do you think people can learn about you (or others) if they get access to your data collected by [APP]?

I will now ask you questions about your understanding of how your data flows within the [APP]'s system. When we talk about data flow, we are talking about how the information that [APP] collects travels from one place to another. There are no right or wrong answers. Please try to use your imagination and think aloud. Do not worry about specific terminology.

3) What happens when you provide your sexual and reproductive health-related data when using [APP]? Where do you think your sexual and reproductive health-related data collected by [APP] is stored, and for how long? *[Give examples of health-related data as mentioned or described by participants in the previous section; e.g., menstrual cycle, sexual activity, etc.]*

4) What do you think the purposes for collecting sexual and reproductive health-related data by [APP] are? *[Remind the types of health data if participants are talking about non-health data]*

a) Do you have any negative feelings about your sexual and reproductive health-related data being collected or used for the purpose(s) you mentioned? If so, what purposes and why?

b) Among the purpose(s) you mentioned, are there any purposes of use you feel comfortable sharing your sexual and reproductive health-related data for, and why?

5) Who do you think has access to your sexual and reproductive health-related data in [APP], if at all?

a) Why do you think those entities have access to your sexual and reproductive health-related data? *[Probe: For what purposes do you think these entities are using the sexual and reproductive health-related data?]*

b) Do you have any negative feelings about your sexual and reproductive health-related data being accessed by any of those entities or someone else for the purposes you mentioned? If so, who and why?

c) In contrast, what entities, if any, do you feel comfortable sharing your sexual and reproductive health-related data with and for what purposes? And why?

6) Overall, do you feel you are able to control or influence how [APP] uses your sexual and reproductive health-related data in any way? If yes, how? If no, why not?

A.2.3 Data Deletion: Beliefs and Experiences of Data Deletion.

1) **Have you ever deleted any of the data collected or used by [APP] or another female mobile health app?** *[If not - skip to the Hypothetical section.]*

[If yes]

a) What data did you delete? *[Probe: Did the data only include what you provided or entered, or other information [APP] could have learned about you?]*

[2] After pilots with participants, we made small changes in the interview guides, such as reordering questions (moving 2.2 Q4 before Q5), and minor clarifications in the wording of several questions (e.g., 2.2 Q5a; A.2.8 Q1; A.2.6 Q4, A.2.6). These changes were minor and did not warrant exclusion of the pilot interviews from the analysis.

b) Why did you delete your data?

c) How did you delete your data? Can you describe the process?*[Probe about sending an email request, having an in-app deletion feature, etc.] [Probe: How easy or difficult was it to delete your data?]*

d) What do you think happened to your data when you deleted it?

e) Do you think there exists a backup of the data you deleted? *[If yes:]*

e.1) What is (are) the purpose(s) for having a backup?

e.2) Did you request a copy of your data before deleting it? Why, and how did you use the copy, if at all?

[If no:] If participants did not delete data collected or used by [APP] or another female mobile health app, ask the following hypothetical questions:

f) What would motivate you to delete data collected or used by [APP]?

g) How would you delete your data? Can you describe the process? *[Probe about sending an email request, having an in-app deletion feature, etc.] [Probe: How easy or difficult would it be to delete your data?]*

h) What do you think would happen to your data when you deleted it?

i) Do you think there would exist a backup of your data if you deleted it? *[If yes:]*

i.1) What would the purpose(s) be for having a backup?

i.2) Would you request a copy of your data before deleting it? Why, and how would you use the copy, if at all?

A.2.4 Privacy Perceptions. Let's talk a little bit more about privacy specifically.

1) Can you explain what the term "privacy" means to you?
2) Is privacy more, less, or equally important to you when using [APP] (or other female health apps) than using non-health-related mobile apps? *[If they ask for examples of non-health related apps, mention social media, gaming, entertainment, financial, productivity apps, etc.]*
3) Have you ever decided not to use, or stop using, [APP] or another female health app because of privacy concerns? *[If yes:]*

a) Could you describe the situation and your privacy concerns? How did you feel about the situation?

b) Have you ever had privacy concerns about [APP] or another female health app but decided to continue using it?*[If yes:]*

b.1) Could you describe the situation and your privacy concerns? How did you feel about the situation?

A.2.5 Opinions about Information Sources. **1) Where or from whom do you learn about the privacy practices of [APP] or female mobile health apps in general? Why?** [*Probe about information provided by [APP], have they ever consulted family members or peers, search engines like Google, online websites, blog posts, news articles, social media sites, government- or state-sponsored sites, app privacy policies, etc.*]
2) In an ideal world, how would you *prefer* to learn about the privacy practices of [APP] or of female mobile health apps in general? *[Probe about sources of information even if they are not currently used or do not even exist.]*
3) Are there any specific sources of information about privacy practices of [APP] or of female mobile health apps in general that you trust or do not trust, and why?
4) How did you use the information you learned? *[Remind participants of the sources of information they mentioned above. Also, probe about specific privacy concerns participants wanted to address.]*
5) Have you shared or would you share the information you learned with someone else, and why?

A.2.6 Perceptions of Data Safety Sections. **1) Are you aware of or have you ever read the App Privacy section or Data Safety section of [APP] on Google Play or the App Store?**

Share the screen and show the label of [APP] to participants. Give them time to read it.

2) What do you think the purpose of this App Privacy / Data Safety section is?
3) Do you find it easy or difficult to understand what this App Privacy / Data Safety section says? *[If they said it's difficult, probe them about what is unclear]*
4) Is there anything that you'd like to change or improve in the App Privacy / Data Safety section? *[Probe: Is there anything that is not mentioned in the App Privacy / Data Safety section but you would like to know more about?]*
5) How did/would you use the information from this App Privacy / Data Safety section?
6) Did reading the App Privacy / Data Safety section change your feelings about the data collected or used by [APP]? If so, how?

A.2.7 Risks. I would like to discuss with you the possibility of potential privacy risks posed by [APP] or female mobile health apps. A privacy risk usually occurs when users' personal data is used or handled in a way that could harm users, including causing emotional, professional, financial, legal, or physical harm. I would like to remind you that you can skip any question you do not feel comfortable answering.

1) Are you aware of any potential privacy risks posed by [APP] or female mobile health apps in general? If so, describe these privacy risks and harm they can cause.
2) Do you think the privacy risks posed by [APP] or female mobile health apps differ across different countries?
3) Are you concerned about these privacy risks? Why, or why not?

A.2.8 Protections. **1) Do/did you take any active steps to protect against the privacy risks posed by [APP] or female mobile health apps? If so, please describe these steps.**
2) Have you ever engaged with the privacy settings or features of [APP], (e.g., looking at the privacy setting page, changing settings, etc.)? If yes, what settings or features have you engaged with? *[Allow participants to answer the question unprompted first, then prompt if needed, e.g., about using strong passwords/PINs,*

turning on anonymous/offline mode, encrypting data, etc.]
3) Do you feel [APP] (or female mobile health apps in general) is (are) still worth using considering the potential privacy risk(s) you described? Why, or why not? *[If participants mention multiple privacy risks, be sure to ask about the trade-off between one risk and another.]*

a) What other methods or tools, if any, do (or would) you use to manage your sexual and reproductive health data? How do (or would) you protect your data when using that method, if at all?

A.2.9 Privacy Legislation. In the next set of questions, I will ask you about privacy legislation as it relates to female mobile health apps. The questions aim to understand your views, not specific knowledge. Please do not worry about specific names or legal terminology.

1) Are you aware of any laws or legal frameworks in your country which manage and protect digital data related to sexual and reproductive health? *[If yes:]*

a) Who do you think these laws or legal frameworks protect? *[Probe about users worldwide, users in specific locations, people using specific apps, companies making apps, etc.]*

b) What protections do you think these laws or legal frameworks offer?

c)To what extent do you feel confident and satisfied that your personal data is protected by these privacy laws? Why, or why not?

2) Assume you live in a state that legally criminalizes abortion and could subpoena the data obtained by these apps to be used as evidence of a terminated pregnancy. Would you trust that existing privacy laws protect your female mobile health app data? Why, or why not?

3) What privacy laws do you think would protect your female mobile health app data? Specifically: a) The country or state you reside in, a citizen of, or just visiting?

b) The country or state where the company that developed the app is registered?

c) The country or state where app data is collected or stored?

d) Other conditions?

A.2.10 Suggestions and Design Recommendations. **1) Based on our discussion, are there any specific features, functionalities, or other measures you would like to see the *developers* of [APP] and other female mobile health apps add to enhance your privacy?** *[These could relate to data collection, usage, storage, and deletion, or any aspect you feel is relevant.]*
2) What other measures would you like *governments and policymakers* to take to address users' privacy concerns with regard to [APP] and other female mobile health apps? *[Probe about desired legal protections]*
3) Would you like to share or discuss any additional thoughts?

B Comparison to Prior Work

Table 1: A comparative table of prior user studies on FemTech privacy

Study	Scope	Methods	Sample	Findings	Recommendations
Cao et al. [16]	Similar to our study, this research explores users' privacy perceptions, practices, and expectations around period-tracking apps. However, while [16] centers on the impact of Roe v. Wade and prosecution risks, our study explores a *broader range of privacy concerns.*	In contrast to [16], which used a vignette-based survey including closed- and open-ended questions about scenarios crafted by the researchers, our study is *qualitative*, grounded in *lived experiences* explored through in-depth interviews with current and past FemHealth app users.	The two studies recruited US participants who self-identified as female, including both transgender and cisgender women, but [16] had a larger sample (N=183) age 19–75 (i.e. including older women who do not menstruate and cannot get pregnant anymore), while our study, due to its qualitative nature, focused on a smaller relevant group age 20–46.	Similar to our study participants in [16] were primarily concerned about data access, with government and law enforcement viewed as most concerning. Our participants were more aware of criminalization risks and more concerned about tracking sensitive data beyond period data including sexual activity and mental health.	[16] suggested future policy considerations such as clarifying law enforcement access and addressing user misconceptions in existing laws like the MBMD Act. Our study advocates for extending privacy protections of sexual and reproductive health information to FemHealth apps and emphasizes the need for federal-level protections.
Dewan et al. [23]	Unlike our study involving *adult* participants' experiences with FemHealth apps, in particular, this study focuses on examining *teenagers'* sexual and reproductive health information seeking behaviors and concerns in a post-Roe world without focusing on a specific source.	Similar to our study, [23] conducted a qualitative study using semi-structured interviews.	In contrast to the 14 *adult* participants in our study, [23] recruited 15 *teenagers* aged 13-17. Similar to our study, participants were residing in the US.	Compared to teenage participants in [23] whose primary concerns were centered on social risks, such as harassment, doxxing, and conflict with family/friends, legal risks was the most prominent concern among our adult participants, followed by data selling and marketing, psychological harm, and stigma.	Although [23] emphasize equipping teens with tools to assess privacy risks, framing reproductive literacy within broader social, cultural, legal, and technological contexts, and urging FemTech to adopt more privacy-protective and culturally sensitive designs, we propose more specific and actionable practical and policy recommendations.
Hudig and Singh [48]	[48] explores user attitudes towards fertility trackers' *data sharing practices*, and offers recommendations for enhancing transparency and user control. While both studies address data-sharing practices, our study explores a *broader range* of privacy topics and practices covering data collection, storage, deletion, risk mitigation, privacy resources, and legal protections.	[48] used a mixed methods approach based on an online *survey* (including Likert-scale questions and scenarios with a fictional fertility tracking company) and *focus groups.* Instead of eliciting opinions about *fictional fertility tracking company*, we explored *lived experiences* with real FemHealth apps.	In contrast to our sample comprised of US current and past users assigned female at birth, [48] recruited 162 *survey respondents of any gender* and four focus groups with 15 participants identifying as women from the *UK, the Netherlands, Mexico, and Spain.*	Similar to our findings, survey respondents in [48] had concerns about data sharing. In contrast to our participants who perceive government access and criminalization as the most prominent risks, respondents in [48] were least comfortable sharing data with employers or advertisers. Findings from focus groups only briefly mentioned concerns about bodily autonomy after the overturning of Roe v. Wade.	Although some collaborative design recommendations to improve transparency and control in [48] overlap with our recommendations, we expand with further actionable, FemHealth-specific measures from our data such as user controls for periodic data deletion, discreet notifications, open-source apps, option for correcting inferences, and contextual privacy alerts.

Study	Scope	Methods	Sample	Findings	Recommendations
Lazarevic et al. [58]	This study explored the perspectives of currently or recently *pregnant participants* on digital pregnancy tools, and their interest in a *hypothetical pregnancy app*, while our study centered on *FemHealth app users* more broadly and explored their *lived experiences* with real FemHealth apps. While [58] revealed some privacy-related findings, its scope was not explicitly privacy-focused.	While [58] took a *mixed methods* approach using a survey and semi-structured interviews, our study focused solely on in-depth semi-structured interviews.	In contrast to our US sample, [58] recruited 108 pregnant participants from *Australia, US, Africa, Europe, and Asia*, and 15 currently or recently pregnant interview participants (10/15 based in Australia).	The majority of survey participants in [58] had privacy and security concerns about pregnancy apps, however, these were *mostly related to remote monitoring* (e.g., self body images sent to healthcare professionals) during the COVID pandemic in 2022. In contrast, US participants in our study, interviewed in 2024, expressed deeper privacy concerns relating to criminalization, harassment, and stigma.	Compared to [58], which briefly emphasized the need for better anonymization and data minimization tools, we propose comprehensive and detailed practical and policy recommendations.
Mcdonald and Andalibi [66]	[66] investigated how individuals who may become pregnant are thinking about privacy of reproductive-related information after the overturning of Roe v. Wade focusing on *broader FemTech*. Our study focused on user privacy in FemHealth apps, in particular. Additionally, [66] placed a specific focus on the *impact of the overturn* of Roe v. Wade as opposed to the wide range of risks explored in our study.	Similar to our study, [66] conducted a qualitative study using interviews.	In [66] interviews were conducted with 15 cisgender women in the US (in the District of Columbia, Oklahoma, and Texas) who were or could become pregnant, but *who do not necessarily use FemHealth apps*. Our sample consisted of *current and past users of FemHealth apps* including one non-binary participant. Our participants resided in different states (except Texas), compared to [66].	The two studies show that concerns about reproductive data privacy vary based on individual risk factors like reproductive age and state of residence. However, our study offers more nuanced, FemHealth app-specific insights, including concerns tied to particular data practices, differences between paid and free apps, FemHealth app-specific user mitigation strategies, and sources of privacy information.	[66] emphasized future research directions, such as identifying and involving privacy intermediaries. In contrast, our work focused on concrete practical and policy recommendations aimed at implementation beyond the research context.

Study	Scope	Methods	Sample	Findings	Recommendations
Mehrnezhad and Almeida [68]	[68] explored participants' privacy understanding across a *broad range of FemTech*, whereas our study focused specifically on *FemHealth apps*.	Compared to our qualitative study, earlier *mixed-methods* research in [68] (conducted in Aug 2021–July 2022) combined an online survey, story completion activity, and individual interviews.	Our sample differed significantly from [68] in terms of *size* (14 v. 5 interview participants) and participant demographics including country (US v. *UK*), *age* (20-46 v. 22-71), and *gender* (individuals assigned female at birth vs. any gender including individuals assigned male at birth).	Participants in [68] mainly voiced concerns about data sharing with third parties, with few mentioning government surveillance unlike in our study, where criminalization was the most prominent concern.	[68] emphasizes a Value Sensitive Design approach, advocating for privacy and security by design, participatory threat modeling, and inclusion of marginalized populations' experiences in system design. In contrast, our study focuses on enhancing user autonomy and transparency through dynamic privacy controls, open-source apps, and legal changes, particularly in light of the data protection–abortion rights.
Salvatore et al. [80]	[80] aimed to assess participants' willingness to use "menstrual cycle (MC) tracking apps" (vs. alternative methods) in research settings and their readiness to share demographic information in a post-Roe v. Wade context. Our study focused on *real-world* privacy experiences with FemHealth apps.	[80] used a *mixed-methods* approach, with qualitative insights being limited to 1 open-ended survey question ("Please indicate why you stopped using a MC tracking app"), as opposed to comprehensive in-depth interviews used in our study.	Both studies focused on US participants. However, our sample was smaller (due to the qualitative nature of the study) and had more narrowed age range (20-46 v. 18-60 in [80]).	Over a third of participants in [80] reconsidered using MC apps after Roe v. Wade was overturned and were unwilling to participate in studies involving daily tracking. In contrast, our qualitative interviews offer deeper insights into privacy concerns grounded in participants' real-world experiences beyond research settings.	Although [80] recommended that policy makers and developers of MC tracking apps should consider ways to safeguard users' personal reproductive health data and reassure them that their health data remain private, our study propose more specific practical and policy recommendations.

Study	Scope	Methods	Sample	Findings	Recommendations
Song et al. [87]	[87] explored how participants understand and perceive *PII*, its sharing, and the risks of its misuse in period and fertility tracking apps. In contrast, our study explored participants' perceptions of *broader data types and practices*, putting stronger emphasis on sexual and reproductive health data as opposed to PII.	Similar to our study, [87] conducted a qualitative study using semi-structured interviews.	Although, our sample size was smaller (14 v. 32 US participants), we only recruited participants who are *current or past users* of FemHealth apps as opposed to [87] where participants with no prior experience of using such app were also included.	The findings of [87] placed greater emphasis on conceptualizations of PII, while our findings focused on perceived privacy risks, mitigation strategies, privacy information sources, and legal protections. [87] reported concerns about legal risks of sharing PII in the post-Roe landscape, personal safety, fraud and identity theft, and unwanted communications and spam. While both studies highlight some overlapping data privacy concerns, our study provides more nuanced insights into the specific implications of risks for sexual and reproductive health data rather than only PII and reveals factors contributing to concerns (e.g., app cost, cross-state differences).	The study recommended that both regulations and industry practices should acknowledge the legitimacy of users' conceptualization and understanding of PII. In contrast, our study offered specific practical and policy recommendations to address participants' concerns.
Song et al. [86]	[86] explored how users on social media collectively make sense of and speculate about privacy risks of period and fertility tracking apps at the *community* level. In contrast, our study explored lived experiences with real FemHealth apps at the *individual* level.	[86] collected and analyzed *social media data* such as Reddit posts. In contrast, we conducted qualitative one-to-one *interviews* with research participants.	In contrast to our study, [86] did *not* have a participant sample. Instead, the authors coded 311 social media threads.	Similar to our findings, [86] found that social media users often speculate about risks of data subpoena and prosecution, surveillance, invasion and harassment, and mental health harms. In addition, our study found that concerns about *selling data* and *sharing data for marketing purposes* persist after the overturning of *Roe v. Wade*. Both [86] and our study reported desire for greater political and regulatory engagement in data protection, yet participants in our study also suggested specific *design recommendations* and recognized more nuanced regulatory gaps, e.g., regarding *minors*.	[86] recommended transparency in privacy communication, regulatory protections, and clear delineation of data ownership. We build on these recommendations by suggesting specific design implementations (e.g., dynamic privacy controls) and policy changes (e.g., the need for federal-level protections).

C Sample of Participants

Table 2: Participant demographics and use of FemHealth apps.

ID	Most used app[a]	App usage	Privacy concern level	State	State stance on abortion	Age	Ethnicity
P1	Fitbit	Past user	High (8 out of 10)	Indiana (IN)	Legally banned	30	Middle Eastern
P2	Kegg	Current user	High (9 out of 10)	Washington (WA)	Legal until viability	35	Asian
P3	Clue	Past user	High (8 out of 10)	California (CA)	Legal until viability	26	Asian
P4	Clue	Current user	High (10 out of 10)	Texas (TX)	Legally banned	28	Black
P5	Flo	Current user	Low (4 out of 10)	New York (NY)	Legal until viability	26	Asian
P6	Clue	Current user	Medium (7 out of 10)	California (CA)	Legal until viability	20	Asian
P7	Apple Health	Current user	Low (3 out of 10)	Missouri (MO)	Legally banned	45	White
P8	BabyCenter	Past user	Medium (5 out of 10)	Texas (TX)	Legally banned	44	Hispanic or Latinx
P9	Clue	Current user	High (8 out of 10)	Alabama (AL)	Legally banned	28	White
P10	Fertility Friend	Past user	High (10 out of 10)	Tennessee (TN)	Legally banned	29	Black
P11	BabyCenter	Past user	Medium (6 out of 10)	Tennessee (TN)	Legally banned	46	White
P12	Apple Health	Current user	Low (1 out of 10)	Texas (TX)	Legally banned	44	White
P13	Flo	Current user	Medium (5 out of 10)	Texas (TX)	Legally banned	23	Hispanic or Latinx
P14	Clue	Past user	Medium (7 out of 10)	Texas (TX)	Legally banned	22	White

[a] Among the users of generic health and wellness apps (e.g., Fitbit and Apple Health), we included only those who reported using the period-tracking and other FemHealth-related functionalities offered by these generic apps.