"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

Jiaxun Cao
jessie.cao@duke.edu
Duke University
USA

Hiba Laabadli
hiba.laabadli@duke.edu
Duke University
USA

Chase Mathis
chase.mathis@duke.edu
Duke University
USA

Rebecca Stern
rebecca.stern415@duke.edu
Duke University
USA

Pardis Emami-Naeini
pardis@cs.duke.edu
Duke University
USA

ABSTRACT

The overturn of Roe v. Wade has taken away the constitutional right to abortion. Prior work shows that period-tracking apps' data practices can be used to detect pregnancy and abortion, hence putting women at risk of being prosecuted. It is unclear how much women know about the privacy practices of such apps and how concerned they are after the overturn. Such knowledge is critical to designing effective strategies for stakeholders to enhance women's reproductive privacy. We conducted an online 183-participant vignette survey with US women from states with diverse policies on abortion. Participants were significantly concerned about the privacy practices of the period-tracking apps, such as data access by law enforcement and third parties. However, participants felt uninformed and powerless about risk mitigation practices. We provide several recommendations to enhance women's privacy awareness toward their period-tracking practices.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; **Usability in security and privacy**; • **Human-centered computing** → *Empirical studies in ubiquitous and mobile computing*.

KEYWORDS

Privacy, Period Trackers, Roe v. Wade

ACM Reference Format:
Jiaxun Cao, Hiba Laabadli, Chase Mathis, Rebecca Stern, and Pardis Emami-Naeini. 2024. "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 (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 22 pages. https://doi.org/10.1145/3613904.3642042

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

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642042

1 INTRODUCTION

The overturn of Roe v. Wade in June 2022 has taken away the constitutional right to abortion in the US, leading to varying levels of abortion limits across different states [12, 44, 60, 78, 107, 119]. This decision jeopardizes reproductive justice and affects millions of women in the US [26], making abortion services much less accessible in many areas, including the 15 states where abortion has been completely banned as of August 2023 [119].

Besides abortion services, women's use of fertility-related technologies can be largely impacted as well, including period-tracking apps – the most popular type of women's mobile health (mHealth) apps [112], as these apps track and collect a vast amount of sensitive data [98], including menstrual cycle data [55, 78, 89], pregnancy [55], sex life [55, 89], and location [55, 89], which can all be used to detect or infer abortions. Worse yet, these highly sensitive personal data are also excessively shared with third parties [32], such as advertisers and insurance companies [55, 89]. Other privacy concerns include lack of readable privacy policies in apps [4, 50, 106], unnecessarily long retention of data [66], and limited user control [66].

Notably, these privacy concerns toward period-tracking apps are even aggravated in the post Roe v. Wade era, as law enforcement can now request fertility-related records from period-tracking app companies as evidence of crimes [98]. For example, a report suggests that 67% of period-tracking apps share data for "legal obligations" [49]. In support of women's reproductive privacy, a term that refers to activities and data relating to women's reproductive health (e.g., pregnancy status) [78], it is crucial to investigate women's privacy knowledge, perceptions, and practices toward period-tracking apps in the post Roe v. Wade context.

A small number of women's health research has focused on menstrual technologies [6, 61, 85, 121, 123]. Attention in this field has been primarily given to menstrual education for adolescents [61, 121, 123], menstrual tracking design [47, 53, 110], and user experiences [42]. However, despite the increasingly concerning data practices, work that investigates the privacy factors of period-tracking apps remains scant, mostly overlooking the impact of abortion-related laws. For instance, two studies conducted outside the US suggested people's lack of privacy awareness when using period-tracking apps [11, 58]. One small-scale interview-based study has

specifically examined how the overturn of Roe v. Wade has impacted women's reproductive privacy practices [78], suggesting participants generally did nothing more than delete their period-tracking app. However, this interview study did not systematically measure the impact of apps' privacy practices (e.g., data sharing stakeholders, type of collected data, and types of user's control) on users' privacy attitudes and concerns. Such feature-level investigations are critical to informing the design of privacy-preserving period-tracking apps and policies.

To fill in this gap, the present paper seeks to answer three overarching research questions (RQs):

- **RQ1**: What factors influence women's privacy perceptions and practices toward period-tracking apps?
- **RQ2**: What are women's knowledge and attitudes toward the overturn of Roe v. Wade and its impact on their privacy concerns and practices of period-tracking apps?
- **RQ3**: What are women's expectations for privacy-enhancing features, actions, and information from stakeholders, such as period-tracking app companies?

To address the RQs above, we conducted a vignette-based study with 183 female participants in the US, evenly distributed in abortion-allowed and banned states. Our findings highlight four critical points: 1) The stakeholders who have access to the period-tracking apps' collected data have the most impact on participants' perceived privacy concerns, with government and law enforcement being the most concerning stakeholders (RQ1); 2) Despite showing significant concerns toward the data practices of period-tracking apps, participants felt uninformed and powerless about strategies to mitigate their privacy concerns (RQ1); 3) Participants were generally unaware of how the overturn of Roe v. Wade might impact their reproductive privacy and their use of period-tracking apps (RQ2); and 4) participants called for app companies and law enforcement to enhance users' control over period-tracking data (RQ3).

Our work makes the following contributions:

(1) Through our quantitative data analysis, we identified the factors that significantly impact women's privacy practices and concerns toward period-tracking apps post the overturn of Roe v. Wade.
(2) Through our qualitative investigation, we surfaced women's privacy knowledge and perceptions toward the period- tracking apps post the overturn of Roe v. Wade.
(3) We provide actionable recommendations for public education, period-tracking app companies, and policies to raise women's reproductive privacy awareness and empower women to have more control over their reproductive data.

2 BACKGROUND AND RELATED WORK

In this section, we begin by presenting the background of the overturn of Roe v. Wade. In addition, a growing body of research in human-computer interaction (HCI) has focused on women's health and menstrual health technologies such as period-tracking apps. We summarize this strand of prior research and highlight how our work can build on existing literature. Last, we dive into how the overturn of Roe v. Wade impacts women's privacy concerns and practices toward period-tracking apps.

2.1 Roe v. Wade and Reproductive Justice

In June 2022, the Supreme Court of the United States decided to overturn Roe v. Wade with the Dobbs v. Jackson decision [78], taking away the constitutional right to abortion. Due to the overturn of Roe v. Wade, state governments now have the full right to decide whether to criminalize abortion or not [78]. As of August 2023, due to political polarization [12], abortion has been completely banned in 15 states [44, 107, 119], while the remaining states legalize abortion with varying levels of protection and gestational limits [60].

The overturn of Roe v. Wade is widely considered a decision that affects the reproductive lives of millions of women in the US and jeopardizes reproductive justice in many ways [26]. For example, policies that restricted access to abortion have constrained reproductive and sexual health services in many ways, including removing public money allocated to abortion facilities and providers [99], criminalizing individuals who provided guidance on self-administered abortions [116], etc. These impacts could be disproportionately more devastating to women from different marginalized and minority groups in the US, such as women suffering from poverty, racism, sexism, etc [23, 26, 99, 116]. It is estimated that there could be a 21% increase in mortality overall, with a 33% increase, particularly for Black women [114, 116].

According to various international human rights organizations, restricting access to safe and legal abortions severely hinders women's rights and health [81, 96]. Unfortunately, while overturning Roe v. Wade is exclusively effective in the US, its impact will be global [26, 116]. Roe v. Wade has been an influential court decision in other countries that have previously achieved progress in reproductive justice, such as Kenya [48]. In Kenya, the High Court of Malindi affirms that abortion access is a fundamental right by referencing Roe v. Wade [48]. Presumably, the Dobbs decision could be as influential as the Roe decision, thereby enhancing reproductive injustice globally. Consequently, it is imperative to (re)investigate protection strategies for women's reproductive health and rights in the post Roe v. Wade context. Our work aims for this goal by looking into the specific privacy implications and proposing protection strategies accordingly.

2.2 Women's Health and Menstrual Technologies in HCI

Motivated by feminist HCI [17, 67, 101], the topic of women's health has been receiving growing attention in the HCI research community over the last several years [6]. At CHI 2017, a workshop on hacking women's health initiated research discussion around women's digital health [15]. Since then, a strand of work has been proliferating, especially relating to intimate and menstrual health [24, 85, 109, 110, 122, 123], maternal health [59, 70, 84, 94], and sexual well-being [33, 63, 64].

Some research in this area has taken the lens of design to explore emerging technologies that promote women's health knowledge and awareness, such as through exploring and testing a wearable e-textile in support of breast self-awareness [5], a design kit with electronic textiles to promote bodily literacy [7], and an augmented system that promotes bodily literacy and pelvic fitness for women [8]. Besides promoting bodily literacy, a volume of work has focused

on designing for women's sexual pleasure [16, 18, 33, 108]. Other work has investigated technologies to increase empathy from partners [69], tools to manage healthcare records across pregnancy [41], and mHealth applications to encourage healthy behaviors for pregnant women [70, 92].

More relevant to our work is a significant focus on menstrual health [6, 85, 123]. For example, in menstrual education, *Help Pinky* is a game developed by Jain et al. [61], teaching adolescent girls in India about menstrual health. Similarly, to encourage discussions on menstrual health between parents and children, Tran et al. [121] developed an internet-connected working model of the uterus. Tuli et al. [123] presented empirical findings from an inquiry into current approaches to educating adolescents about menstruation, suggesting gaps between parents' and teachers' expectations. Besides education, prior work has explored menstrual tracking [42, 47, 53, 110]. For instance, recent studies have investigated using ambient light and color-emitting smart mirrors to track menstrual information [47, 53]. Similarly, Epstein et al. [42] have examined the practices and motivations of using menstrual tracking apps in the US, suggesting design drawbacks and the non-inclusive nature of the menstrual tracking apps.

Although the prior research has shed light on the significance and benefits of promoting women's health through various technologies, work that empirically investigates the concerns, such as privacy factors of menstrual technologies, remains nascent. However, menstrual technologies track and collect a variety of sensitive data such as sexual activities and medical records without many regulations in the US [78], depriving women of their reproductive rights and freedom [9, 10]. More of such privacy concerns will be detailed in Section 4.2, where we narrow down our focus on one of the most widely used menstrual technologies – period-tracking mobile apps, with 26.60 million users worldwide in 2022 [112]. To promote women's reproductive health and justice, it is equally vital to look into the benefits, as well as the potential harms of these menstrual technologies. While most of the work exploring menstrual technologies in HCI has been focusing on usability, our work highlights the privacy harms and how women users perceive or neglect the harms at a critical historical moment – the overturn of Roe v. Wade.

2.3 Privacy Concerns of Period-Tracking Mobile Apps in the Post Roe v. Wade Era

Scholarship investigating the privacy practices of mHealth apps in general, and period-tracking apps in particular, has more often than not yielded concerning findings. For instance, sensitive data, including reproductive-related behavior and location data, is collected by women's mHealth apps. In a scoping review of 23 popular women's mHealth apps, it was found that all apps permitted behavioral tracking, while 61% allowed location tracking [4]. The same study has found that a significant 87% of these apps share the collected data with third parties [4].

Despite their concerning data practices, prior work has shown that 30% of period-tracking apps did not display any privacy policy [4]. Similarly, a comprehensive analysis of 20,991 general mHealth apps revealed that 28.1% of the apps provided no privacy policy at all [117]. Even when privacy policies are available, questions rightfully arise regarding their effectiveness. Despite its sensitivity, reproductive-related data is often not covered by privacy policies or even completely disregarded [106]. In addition, Fowler et al. assessed that understanding a period-tracking app's privacy policy or terms of service typically requires a college-level education. This suggests that most American users may not fully understand how their data is being used and shared [50]. That is, if they even read it at all, only a mere 9% of American adults consistently read privacy policies before agreeing to them [14].

Privacy and data practices of period-tracking apps are especially concerning as the information collected by health-focused apps is not covered by the Health Insurance Portability and Accountability Act (HIPAA) [102]. Likewise, in the UK and European Union (EU), it is unclear whether female-oriented technologies (FemTech) data is protected under the "special category data" in the General Data Protection Regulation (GDPR) framework in the EU and if such data fall under "medical" category or other groups in the UK Medicines and Healthcare Products Regulatory Agency (MHRA) [43, 79, 80]. Essentially, women's health data protection has been poorly defined in many major legal frameworks worldwide, and the responsible stakeholders remain unknown [80].

With the overturn of Roe v. Wade and the resulting changing legal landscape, interest and concern surrounding the privacy of period-tracking apps have naturally risen. The number of articles about the danger of using women's mHealth apps and privacy-related reviews has increased [32]. Mozilla has labeled 18 of 25 popular period- and pregnancy-tracking tech with a "privacy not included" warning [83]. A report by the Organization for the Review of Care and Health Apps (ORCHA) revealed that 67% of the period-tracking apps tested share data for "legal obligations" [49], which is particularly alarming in the current context of the US abortion laws.

The extent to which these practices represent a real threat remains a topic of ongoing debate. The Electronic Frontier Foundation (EFF) argues that although anyone may buy certain period-tracking apps' datasets, it is not the primary strategy being used to criminalize abortion seekers, at least not currently [51]. Presently, law enforcement relies on text messages, emails, and browser search histories [57]. Indeed, in 2022, a Nebraska police officer used Facebook messages to investigate an alleged illegal abortion [65]. In another case, a visit to a web page titled "National Abortion Federation: Abortion after Twelve Weeks" has been used to prosecute a woman in Indiana [128]. Nevertheless, the fact remains that fertility apps are not entirely safe to use. The Federal Trade Commission (FTC) filed a complaint against Flo Health Inc. (the most downloaded period-tracking app worldwide in 2022 [111]), accusing them of allegedly sharing users' sensitive health data with Facebook, Google, AppsFlyer, and Flurry over an extended period of time while they explicitly told their users they did not [27]. The complaint resulted in a settlement and the app introducing an "Anonymous" mode, but research shows that de-identification measures are rarely reliable [100]. More recently, the FTC charged another period-tracking app, Premom, for deceiving users about their data practices by disclosing health data to third parties [28].

While considerable attention has been given to user experiences and app practices, little work has been done to understand users' privacy perceptions surrounding period-tracking apps, particularly

following the overturn of Roe v. Wade. A study done in New Zealand revealed most participants regard the data collected by period-tracking apps as uninteresting and unproblematic [58], supporting the use of their menstrual data in academic research [58, 106]. By contrast, a poll by the Information Commissioner's Office (ICO) in the UK revealed that women had greater concerns about data transparency and security than ease of use and costs of period-tracking apps [1]. Building on this finding, another UK-based study suggests that users lack the technological skills to protect their FemTech data despite the privacy concerns expressed [80]. Another study conducted in Germany suggested that the perceived benefits of period trackers outweighed the perceived harms among users. In fact, while non-users frequently expressed privacy concerns when it came to sharing intimate data with period trackers, the interviewees who were actively using the apps rarely raised such concerns themselves [11].

Collectively, these studies have revealed an important fact – the privacy paradox phenomenon may widely exist in period-tracking apps, similar to other mHealth applications [125, 129]. By definition, *privacy paradox* refers to the contradictory privacy concerns expressed by users and their actual behaviors, e.g., voluntarily giving away information, making little effort in data protection, etc. [52]. One of the widely used explanations for privacy paradox is *privacy calculus*, which refers to users' comparison between the perceived privacy risks and their anticipated return for revealing information, e.g., the utility of apps [46, 105]. How users weigh the privacy risks and benefits of mHealth apps depends on various contextual factors, e.g., type of requested data, type of device, etc. [45]. In more sensitive contexts, such as sexual and reproductive health interventions, the privacy of information- and support-seeking methods afforded by mHealth technologies have greatly attracted users' interest [45, 115]. For instance, in a study of mobile cell phone-based HIV prevention intervention, Cornelius et al. [30] showed that the confidentiality of the technology was perceived as an advantage for seeking HIV-related information.

The majority of existing literature on users' privacy perceptions toward period-tracking apps has been conducted outside the US, where the legal landscape surrounding abortion differs. More recently, McDonald and Andalibi interviewed 15 individuals who may get or were pregnant in the US to understand how the overturn of Roe v. Wade impacted their reproductive privacy practices, and they nearly all reported deleting period-tracking apps without taking further action [78]. They also found that participants' reproductive risk, age, location, and experience with oppressive government could potentially have an impact on participants' privacy strategies. Due to its qualitative nature, this study was not able to quantitatively measure the impact of various in-app privacy factors (e.g., type of requested data [45] and users' data autonomy [125]) on users' attitudes and practices toward period-tracking apps. Such investigation is critical to informing the design of period-tracking apps and policies to protect women's privacy more effectively.

To shed light on the privacy attitudes and expectations of female users of period-tracking apps, we conducted a large-scale survey. Through careful quantitative and qualitative investigation, we identified the specific factors that have a significant impact on women's privacy concerns and practices toward period-tracking apps post the overturn of Roe v. Wade.

3 METHODOLOGY

To surface the factors that influence women's privacy attitudes, concerns, practices, and expectations toward period-tracking apps post the overturn of Roe v. Wade, we conducted an online vignette study with 183 Prolific[1] participants from the US. We presented each participant with a consent form at the beginning of the survey.

3.1 Fractional-Factorial Vignette Study

Leveraging short hypothetical scenarios, vignette-based studies aim to elicit participants' considerations and judgments toward the presented scenarios [13, 77, 86]. By researching theoretically important factors and systematically varying these factors [13], multiple vignettes are presented to participants. In a fractional-factorial vignette study, each participant only answers questions about a subset of scenarios to ensure the response quality within reasonable survey completion time [13].

Previous privacy research [35, 37, 39, 71, 72, 76, 77, 86, 95, 127] has extensively used the vignette technique to examine privacy norms in varying privacy-related contexts. As opposed to testing for a static definition of privacy [77], the vignette technique can help identify the relative importance of each privacy factor that participants take into consideration when making a privacy decision within a specific community [62, 126].

3.2 Study Design

3.2.1 Factor Specification. We quantified the impact of four privacy factors (e.g., **Data Storage**) in our study. For each factor, we considered multiple levels (e.g., **Data storage: Device**, **Data Storage: Cloud**) to test a hypothesized range of privacy protection, from low-protective (e.g., **Data Storage: Cloud**) to high-protective (e.g., **Data storage: Device**). We only included privacy factors and levels that prior research has identified as potentially important in users' privacy attitudes toward period-tracking technologies (e.g., period-tracking apps, FemTech) (Table 1). We included the following four factors in each vignette:

- **Collected Data**: The type of data the period-tracking app collects (five levels).
- **Data Storage**: The location where the collected data is being stored (two levels).
- **Data Sharing**: The stakeholder that the data is being shared with (five levels).
- **User Control**: The type of controls users have about their collected data (three levels).

To design vignettes that are realistic and similar to the current data practices of period-tracking apps, we set the **Menstrual cycle data** as the default level (most protective) of the **Collected Data** factor. We considered collecting additional data types less protective and hypothesized that participants would become more concerned if the period-tracking apps collected data types in addition to menstrual cycle data. To test this hypothesis, we tested four additional data types (precise location, mental health data, physical health data, and intimacy data), which have been shown to impact privacy concerns and practices toward period-tracking technologies in prior work (Table 1).

[1] https://www.prolific.co/

Factor	Level and Example References
Collected Data	Menstrual cycle data (e.g., days bleeding) [4, 78, 89, 106]. Menstrual cycle data (e.g., days bleeding) & Precise location [4, 31, 55]. Menstrual cycle data (e.g., days bleeding) & Mental health data (e.g., moods, feelings) [4, 55, 73, 106]. Menstrual cycle data (e.g., days bleeding) & Physical health data (e.g., body pains, weight) [75, 106]. Menstrual cycle data (e.g., days bleeding) & Intimacy data (e.g., intimate relationships, sexual activities) [98, 106].
Data Storage	Device [93, 98, 120]. Cloud [93, 98, 120].
Data Sharing	App company [55, 89, 97, 98]. App company & Law enforcement officers [78, 89, 106]. App company & Third party advertisers [4, 55, 89]. App company & Health care providers (e.g., OBG-YN, primary care physician) [4, 89]. None
User Control	Opt out from data sharing [55, 93]. Data deletion [90, 93]. None

Table 1: Each vignette in the survey included the four factors (e.g., collected data). For each factor, we selected a random level (e.g., menstrual cycle data) among the possible levels.

Sharing data with the app company is a common practice for period-tracking apps [55, 89, 97, 98]. Therefore, we identified **App Company** as the base level of the factor **Data Sharing**. We tested three additional data-sharing parties (law enforcement officers, third-party advertisers, and healthcare providers), which were shown to have varied privacy implications (Table 1). We considered no data sharing as the most protective level.

Cloud storage could expose people to higher privacy and security risks compared to device storage, and people are more concerned about cloud storage as opposed to data being stored on the device [93, 98, 120]. To test this in the context of period-tracking apps post the overturn of Roe v. Wade, we considered two levels for the factor **Data Storage** – cloud and device.

Based on prior research, users would like more control over their data when interacting with digital technologies [80]. In our survey, we tested participants' attitudes toward three levels of user control: opt-out from data sharing, data deletion, and no control over data. These levels were identified by the prior work to potentially impact privacy concerns and attitudes toward data-intensive technologies and apps [55, 90, 93].

3.2.2 Scenario Design. Using the factor levels (e.g., Collected Data = Menstrual cycle data), there are 150 possible combinations. After eliminating unrealistic options, such as scenarios with **Data Sharing** = **None** ("Your data will not be shared with anyone.") and **User Control** = **Opt out from data sharing** ("You have the option to opt out of your data being shared outside the app company."), 75 scenarios remained. In the survey, each vignette presented the factors in this order: **Data Type**, **Data Storage**, **Data Sharing**, and **User Control**. Each participant was presented with four randomly selected scenarios. We selected four, as our pilot study showed that having four scenarios would allow participants to complete the survey in less than 15 minutes. The following is an example of a scenario that we presented to participants:

> Imagine you are looking for a period-tracking app to install on your phone to keep track of your menstrual cycle. You see a period-tracking app with the following data practices: The app **only** collects your **menstrual cycle data** (e.g., days bleeding). This app will **store** your data on the **device**. Your data **will not be shared** with anyone. You have **the option to delete your data**.

3.2.3 Survey Design. We implemented our survey on Qualtrics[2]. We started the survey with a consent form. We then presented participants with instructions on the survey procedure. Participants were randomly assigned to see four period-tracking apps' data collection and use scenarios. At the end of each scenario, we asked participants some follow-up questions.

First, we asked participants to specify their level of concern toward the presented scenario's data practices and the reason(s) behind their response. Next, to assess participants' attention, we presented an attention-check question. The attention-check question was a multiple-choice question where we asked either about the type(s) of data being collected in the given scenario, where the collected data is being stored in the given scenario, with whom the data is being shared in the given scenario, or what data control users have in the given period-tracking scenario. For each scenario, we randomly selected one type of attention-check question. When analyzing the data, we removed participants who missed more than two attention-check questions from the database for further analysis.

After the scenario questions, we asked participants about their period-tracking app usage, such as their period-tracking tool usage history and purposes of usage. Then, we asked participants about their concerns and risk mitigation practices toward the period-tracking apps that they have used. We then asked participants about their knowledge of the data practices of period-tracking apps.

[2]https://www.qualtrics.com/

Next, we asked participants questions focused on the overturn of Roe v. Wade. We started by asking participants about their familiarity with the overturn and their concerns about the overturn of Roe v. Wade. Then, we asked participants to specify how much impact they believe the overturn of Roe v. Wade has had on their privacy concerns about the data practices of period-tracking apps and their rationales. We also asked participants if they had ever changed their period-tracking habits and practices due to the overturn of Roe v. Wade. We ended the survey with demographic questions. See the complete survey questions in Appendix A.

3.3 Pilot Survey

Before launching the formal survey, we conducted a pilot study with 20 Prolific participants. Based on the timing findings of the pilot survey, we reduced the number of presented vignettes from six scenarios (average completion time of 31 minutes) to four scenarios for our main survey (average completion time of 14 minutes).

3.4 Participant Recruitment

We initially recruited 200 participants on Prolific. Participants were required to be 1) at least 18 years old, 2) living in the United States, 3) self-identified as a female, including transgender and cisgender females, and 4) having an approval rate of over 95% on Prolific. To investigate differences between participants from abortion-banned states and abortion-allowed states (according to the latest data from [119] as of Aug 2023), we recruited half of our participants from 15 abortion-banned states (e.g., Texas), while the other half were recruited from 8 abortion-allowed states, with no gestational limit (e.g., Minnesota). On average, it took 14 minutes for participants to complete the survey. Upon completion, each participant received a 4 USD compensation.

3.5 Data Analysis

3.5.1 Quantitative Analysis. For the quantitative analysis, we statistically modeled participants' self-reported privacy concerns toward period-tracking apps' data practices presented in vignettes. Since the possible responses to the concern question were ordinal categorical (e.g., slightly concerned, somewhat concerned), we conducted an ordinal regression analysis by constructing a cumulative link mixed model (CLMM). We selected a mixed model as our survey had a repeated-measure design, where each participant was asked the same question about their level of concern regarding four vignettes. To count for potential within-participants data dependencies, we constructed a mixed regression model with random intercept (CLMM).

Using the Akaike Information Criterion (AIC) as the metric for the model's goodness of fit, we performed model selection with forward addition. For the model selection, we considered the four scenario factors (Table 1), the order in which we presented the scenarios (**Scenario Order**), the demographic factors, and the first-order interaction terms.

For each factor, we selected one level as the baseline. For example, for **User Control**, we selected *None* as the baseline. It is important to note that any level of each factor can be selected as the factor's baseline, and the selection of baseline does not have any impact on the relative importance of the levels of factors. Table 3 shows the explanatory variables that we included in the final regression model after the AIC model selection process.

In the following, we provide details regarding the CLMM we employ for inference. Consider the i_{th} participant in our survey, p_i. Concern levels for the j_{th} app p_i sees can be represented as $Y_{i,j} \in \{1, 2, 3, 4, 5\}$. For $y \in \{1, 2, 3, 4\}$, the probability that the concern level of p_i is at most y is modeled as

$$\Pr\left[Y_{i,j} \leq y\right] = \sigma\left(\alpha_{y|\,y+1} + \mu_{p_{i,j}} - \hat{\beta}^T p_i\right),$$

where $\sigma(\cdot)$ is the sigmoid function, $\alpha_{y|\,y+1}$ is the threshold parameter between the class y and $y+1$ determined by the model, and μ_{p_i} is the random effect modeled as a Gaussian with zero mean and constant variance σ^2_μ. $\hat{\beta}$ is the model's estimates for $(\beta_1, \ldots, \beta_p)$, and p_i is the observed demographic and app attribute data for participant i.

3.5.2 Qualitative Analysis. For open-ended survey questions, we conducted a qualitative content analysis [103]. One of the authors first annotated and coded 20 responses (10% of our total responses). According to the annotations, the author constructed a codebook to analyze the remaining responses. Two researchers independently applied the codebook to the responses and iteratively revised the codebook through several meetings. After resolving the coding discrepancies and disagreements, we reached a Cohen's Kappa intercoder agreement of 87.5%, which is considered "almost perfect" [19]. The resulting codebook contains 10 main codes, 55 sub-codes, 101 sub-sub-codes, and 9 sub-sub-sub-codes. The final codebook is available in Appendix B.

3.6 Ethics and Positionality

3.6.1 Ethical Statement. The study has been approved by the university's Institutional Review Board (IRB). In addition, prior to the start of the survey, each participant was informed of the study procedure, risks, compensation, confidentiality, voluntariness, and rights to contact. All participants read and agreed to our terms before participation.

3.6.2 Positionality Statement. In qualitative research with respect to marginalized groups such as women, it is crucial to clarify researchers' positions in society and their identities [104]. Researchers' positionalities such as class, gender, and race could invariably impact the research process and outcomes [40, 91]. In this work, four out of five authors are cisgender females, and three of us were located in the US when conducting the research, making most of us part of the same marginalized group described in this study, i.e., women in the post Roe v. Wade US. Therefore, our identities and personal experiences informed the design of the survey questions that our participants could relate to. Additionally, when conducting the qualitative analysis, our identities helped us resonate with participants' privacy concerns.

3.7 Limitations

Our study employed a vignette-based approach to understand how different privacy practices of period-tracking apps may impact individuals' privacy concerns, attitudes, and practices. To limit the survey length for response quality, we only tested a limited range of

Age		State		Race			Political Affiliation			Degree		
Range	19-75	Legal abortion state	51.37%	White	73.8%	(75.5%)	Democrat	52.5%	(39%)	Bachelor's degree	33.3%	(22.8%)
Mean	39.05	Full abortion ban state	47.54%	Black or African American	4.9%	(13.6%)	Independent	21.8%	(30%)	Some college credit, no degree	26.8%	(16.6%)
STD	12.34	Prefer not to say	1.09%	Asian	3.3%	(6.3%)	Republican	17.5%	(28%)	High school diploma, GED, or alternative	13.1%	(28%)
Median	36.0			Hispanic or Latino, or Spanish Origin of any race	2.7%	(19.1%)	None	3.8%		Associate's degree	12.0%	(10.7%)
US Median	38.9			American Indian or Alaskan Native	1.6%	(1.3%)	Other*	2.2%		Master's degree	9.3%	(10.6%)
				Prefer not to say	1.1%		Prefer not say	2.2%		Doctorate degree	2.7%	(1.7%)
				Multiracial	12.6%					Professional degree beyond bachelor's degree	1.1%	(1.2%)
										12th grade—no diploma	0.6%	
										Prefer not to say	1.1%	

Table 2: Demographic breakdown of survey participants. Note that for race, participants were able to select multiple answers. The political affiliations of the people who selected 'other' are either 'anarchist', 'green', 'leftist', or 'Marxist-Leninist.' In the Race and Degree columns, the numbers in parentheses show the US average for women, according to census data from 2022 and 2023 [21, 22]. In the Political Affiliation column, the numbers in parentheses show the US average for women, according to Pew Research Center data from 2020 [25].

data practices identified by prior work to impact users' privacy attitudes and concerns. Future work could expand the factors and their levels to evaluate more period-tracking scenarios, such as sharing period-tracking data for analytics and academic purposes [106].

In addition, while vignettes help isolate specific factors and their levels, it should be noted that they may not fully illustrate the complexity of real-life behaviors. Thus, participants' reactions to these scenarios might differ from their real-life actions. To make the scenarios as realistic as possible, we included privacy factors and levels similar to data practices of period-tracking apps. In addition, we included participants' free texts in our in-depth qualitative analysis to better reflect participants' lived experiences [74].

While most period-tracking app users are female, we acknowledge that other populations use period-tracking apps, e.g., male partners [87, 118]. Partners' use of period-tracking apps, such as for intimate surveillance [118], supporting their female partners [3, 54], and increasing chances of conceiving [82], may violate women's privacy by disclosing their reproductive information without women's knowledge or permission, i.e., interdependent privacy (IDP) violations [87]. In this study, we focused on how period-tracking apps are approached by users who use such apps for their own reproductive health [78]. Therefore, we only recruited female participants. However, considering the potential existence of IDP violations in period-tracking apps, we encourage future work to investigate other users' (e.g., partners) perspectives, especially if their app activity would put women at risk.

Participants were recruited through the Prolific platform, which may introduce biases relating to the characteristics of its users. In addition, our participants are not entirely representative of the U.S. population. For instance, only 4.9% of our participants identified as Black or African American alone, compared to the U.S. Census estimate of 13.6%. Those identifying as Hispanic or Latino only constituted 2.7% of our sample (U.S. Census reports 19.1%).

4 RESULTS

We initially recruited 200 participants from the Prolific platform, who identified themselves as women. In our survey, we presented four randomly selected vignettes to each participant. For each scenario, we asked one attention-check question to assess participants' understanding of the data practices described in the scenario (Section 3.2.3). In data analysis, we excluded participants who (1) got at least 3 attention-check questions wrong, (2) did not give full consent, or (3) were not in completely abortion-allowed or banned states (e.g., Virginia). As a result, we removed 17 responses. We report our findings from 183 participants. The average age of our participants was 39 years old. We recruited a balanced sample of participants who live in states where abortion is banned (87/183, 48%) and states where abortion is legal with no gestational limit (94/183, 51%). We summarize our participants' demographic information in Table 2. Complete demographic information can be found in the Appendix C.

4.1 Participants' Attitudes And Usage Toward Period Tracking

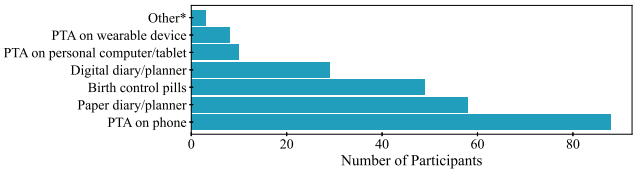

Figure 1: Distribution of participants by period-tracking tool used. Note that participants were able to select multiple answers; thus the sum of participants in the figure may not sum up to 183. Among the 3 participants who indicated using an alternative period-tracking method, one reported relying on an IUD, the others reported keeping mental notes of period dates or using the notepad app on a computer.

Period-tracking apps are the most common tool to track upcoming periods. 67% of our survey participants (123/183) reported that they are currently tracking their periods or have previously tracked their periods. The predominant choice for about 51% of our participants (94/183) to track their periods was using period-tracking apps, mainly Flo, Period Tracker Period Calendar, Apple Cycle Tracking, and Clue. Other frequently mentioned methods were using a paper diary or calendar (58/183, 32%) and using birth control pills (49/183, 27%). Preparing for upcoming periods emerged as the most common purpose for using a period-tracking app (81/183, 44%). Other commonly mentioned purposes included

becoming aware of how the body is doing (40/183, 22%) and tracking fertility (35/183, 19%).

Desire to download period-tracking apps varies depending on who is recommending. We asked participants to rate their likeliness of downloading a period-tracking app recommended by different stakeholders (Table 2). 82% of participants (150/183) reported being not at all likely to trust an app recommended by government and law enforcement officers. Similarly, most participants were not likely to download a period-tracking app recommended by their employers (137/183, 75%) or insurance companies (99/183, 54%).

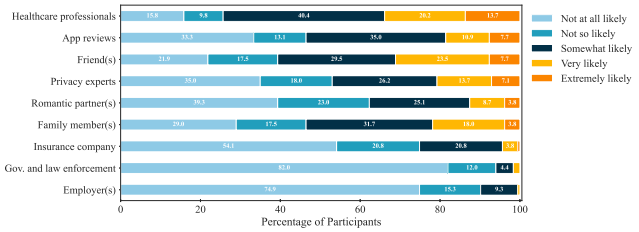

Figure 2: Distribution of downloading a period-tracking app based on different stakeholders' recommendations. Ordered by 'Extremely likely' Ratings.

However, 74% of our participants (136/183) were at least somewhat likely to accept the app recommendations from healthcare professionals. Likewise, 53% of participants (98/183) showed at least some receptiveness to downloading an app recommended by family members. Interestingly, participants showed relatively low receptivity to downloading an app recommended by romantic partners, as 39% (72/183) reported to be not at all likely to do so.

4.2 Factors That Influence Privacy Concerns Toward Period Tracking (RQ1)

We asked participants to rate their concerns regarding using various period-tracking methods. Notably, they were most concerned by the privacy implications of posting on social media about fertility-related topics. Using period-tracking apps either on a wearable device, a personal computer/tablet, or a phone generated similar levels of concern, indicating that the choice of devices did not significantly impact their privacy concerns (p-value > 0.05).

Participants showed relatively lower levels of concern regarding the privacy implications of searching for period-tracking-related information online or engaging in discussions through communication platforms (e.g., WhatsApp). This observation is noteworthy, especially considering that it is the strategy law enforcement currently relies on to criminalize abortion seekers [57]. Full results are shown in Figure 3.

To gain deeper insights into the specific data and privacy practices contributing to participants' privacy concerns, each participant was presented with four randomly selected period-tracking app scenarios. Based on the Akaike Information Criterion (AIC) of the CLMM regression model, the party with whom the data is being shared with (**Data Sharing**) was the most important factor

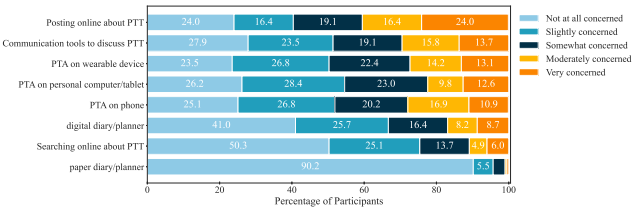

Figure 3: Distribution of privacy concern levels towards different period tracking practices. Ordered by 'Very concerned' Ratings. PTA here refers to period-tracking apps, while PTT refers to period-tracking and fertility topics.

to explain participants' privacy concerns. The second most important factor was the type of controls users have regarding their data (**User Control**). The type of data collected by period-tracking apps (**Collected Data**) was the third most impactful factor, and where the collected data is being stored in (**Data Storage**) was the least important factor in explaining participants' level of privacy concerns toward period-tracking apps. In the remainder of this section, we describe the surfaced themes. When providing a quote from our participants, we include the state where participants live and indicate whether the state legalizes abortion or not using B (banned) and L (legal), e.g., Minnesota, L.

Data being shared with law enforcement is most concerning. Compared to data not being shared with any parties, participants were most concerned about data being shared with *government and law enforcement officers* (row 7: estimate = 4.54, p-value < 0.001). Data being shared with law enforcement officers significantly increased participants' level of privacy concerns even when the described period-tracking apps offered the control to the user to delete their collected data (row 21: estimate = 1.75, p-value < 0.05).

When asked to specify the reasons for the level of concern, 37% of participants (67/183) indicated that they perceived their personal data being shared with government and law enforcement officers "unacceptable," especially when it comes to data as sensitive as menstrual cycle data. 33% of participants (22/67) added that they were confused about why law enforcement officers would need menstrual cycle data. P38 said:

> Sharing personal information of this nature with law enforcement is unnecessary, not to mention incredibly wrong. (Alabama, B)

According to P38, the confusion caused by unnecessary data sharing led to their distrust of the app. Importantly, app companies should earn more users' trust by restricting their data sharing with unnecessary third parties that do not directly benefit users' goals of using period-tracking apps.

Besides the lack of necessity, another expressed concern for sharing data with law enforcement was due to "the current political climate in the US." Notably, only 8% of participants (14/183) attributed their privacy concerns to the overturn of Roe v. Wade. P110, who terminated the use of period-tracking apps indefinitely, mentioned:

> I decided last year, after the overturn of Roe v. Wade, to quit tracking my data completely and decided never

Row	Factor	Level of Concern (AIC = 1864.70)			
		OR	β	Std. Error	p-value
	Collected Data (baseline = Menstrual cycle data)				
1	Location Data	5.562	1.72	0.298	***
2	Intimacy Data	5.238	1.66	0.352	***
3	Mental Health Data	2.314	0.839	0.292	**
4	Physical Health Data	1.498	0.404	0.316	0.2
	User Control (baseline = None)				
5	Control Delete	0.08	-2.52	0.313	***
6	Control Share	0.289	-1.24	0.617	*
	Data Sharing (baseline = None)				
7	Law Enforcement	93.317	4.54	0.714	***
8	Third Parties	26.762	3.29	0.641	***
9	Healthcare Providers	7.367	2.00	0.610	**
10	App Companies	4.549	1.52	0.484	**
	Data Storage (baseline = Device)				
11	Cloud	0.833	-0.183	0.449	0.683
	Education Level (baseline = No Degree)				
12	Degree: Prefer not to Say	13.45	2.60	1.66	0.118
13	Bachelor's Degree	3.892	1.36	0.421	**
14	Graduate Degree	2.519	0.924	0.544	0.089
15	Associate's degree	1.161	0.149	0.562	0.791
	Political Party (baseline = Democrat)				
16	Republican	3.04	1.11	0.513	*
17	Independent	0.986	-0.014	0.388	0.971
	Age (numeric)				
18	19,...,75	1.014	0.0144	0.0161	0.373
	Data Sharing (baseline = None) : User Control (baseline = None)				
19	App Companies : Control Delete	1.956	0.671	0.517	0.194
20	Healthcare Providers : Control Delete	17.082	2.84	0.749	***
21	Law Enforcement : Control Delete	5.755	1.75	0.816	*
22	Third Parties : Control Delete	2.659	0.978	0.745	0.189
23	Healthcare Providers : Control Share	1.10	0.0956	0.810	0.906
24	Law Enforcement : Control Share	1.23	0.206	0.889	0.817
	Scenario Order (baseline = Scenario 1)				
25	Scenario 2	1.33	0.287	0.252	0.255
26	Scenario 3	1.55	0.438	0.265	0.0988
27	Scenario 4	1.09	0.0894	0.288	0.756
	Threshold Coefficients				
28	$\alpha_{4\|5}$	-	0.851	0.740	-
29	$\alpha_{4\|5}$	-	2.59	0.741	-
30	$\alpha_{4\|5}$	-	4.08	0.745	-
31	$\alpha_{4\|5}$	-	5.43	0.756	-
	Random Effects				
32	σ^2_μ	-	4.170	-	-

Note: $^{*}p < 0.05$ $^{**}p < 0.01$ $^{***}p < 0.001$

Table 3: CLMM regression model to describe how various scenario factors impact participants' level of privacy concerns toward period-tracking data collection and use. Each row corresponds to a single factor and shows the resulting model estimate, i.e., the coefficient, for that factor. The odds ratios are ranked in descending order according to their effect size, represented by the magnitude of the model coefficients (β). A positive estimate for a factor-level (e.g., Collected Data: Intimacy Data) implies that transitioning from the baseline of the corresponding factor (e.g., Menstrual Cycle Data) to that level of the factor (e.g., Intimacy Data) would increase the perceived level of concern. A negative estimate reflects the opposite of this trend. In addition, we included the AIC value for the model, which represents the model's goodness of fit.

> to reuse any tracking apps. The safety and reproductive freedoms in the US are simply too uncertain and dangerous, and although I trust Planned Parenthood, I don't trust the government or some other apps and I am uneasy about my data ever getting shared with anyone or anything else. (Minnesota, L)

Since participants saw period-tracking app-related questions before we gave them the context of the overturn of Roe v. Wade as described in Section 3.2.3, we did not prime participants with the influence of Roe v. Wade. As a result, to some extent, the low percentage of overturn-related responses speaks to the general unawareness of the association between period-tracking apps and the overturn of Roe v. Wade among participants.

Concerns toward potential harms caused by third parties accessing period-tracking apps' data. Third parties were the second most concerning stakeholder to have access to the period-tracking data (row 8: estimate = 3.29, p-value < 0.001). 31% of participants (57/183) mentioned that they were concerned about how third parties including advertisers and insurance companies could use the period-tracking apps' data against them. P116, who reported to be strongly concerned about data being accessed by insurance companies, said:

> I suppose some companies and entities could use your negative health history in negative ways like insurance companies charging more because of pre-existing conditions. (Oregon, L)

With that said, concerns toward third parties can be more persistent than other concerns due to commercial profits. As participants like P116 strongly suspected third parties would benefit hugely from users' period-tracking data, it would be harder for app companies to dispel users' doubts, even with opt-out guaranteed. P105 mentioned:

> This app does say they will not share my data with anyone, but I wonder if any of my information may be shared without my knowledge. (New Mexico, L)

Similar to P105, 11% of participants (21/183) explicitly said that app companies might still share their data despite opt-out. Consequently, app companies must put in more effort to convince users of the effectiveness of their data protection practices instead of simply giving users an opt-out option without further and valid illustrations.

Privacy calculus in data sharing with health professionals. The second least concerning type of data-sharing stakeholder was healthcare providers (row 9: estimate = 2.0, p-value < 0.01). 10% of participants (19/183) stated healthcare professionals having access to be beneficial for their health goals. P36 mentioned:

> If the only one shared with was my own doctor, then it would probably be a good app to have, as it helps keep your doctor included in your health goals. (Wisconsin, B)

In essence, when participants' needs for such healthcare goals outweigh their privacy concerns, they prefer sharing data, indicating the existence of privacy calculus [46, 105] in period-tracking app usage. However, compared to data not being shared with anyone, 9% of participants (17/183) were still significantly concerned (row 9: estimate = 7.37, p-value < 0.01) about their data being shared with healthcare providers, even if they were being offered the option to delete collected data (row 20: estimate = 2.84, p-value < 0.001). Among these participants, five explicitly mentioned their desire to have more control over specific types of data to be shared with health professionals. Hence, a granular sharing setting is important in respecting users' different privacy calculus perceptions (detailed in Section 5.3).

Participants are least concerned when data is being shared within the app company only, despite some reservations. In comparison, participants were least concerned about sharing data with the app company only (row 10: estimate = 1.52, p-value < 0.01). However, in qualitative responses, participants still demonstrated concerns about data sharing with app companies. 19% of participants (34/183) mentioned concerns toward app companies' data security practices. P30 mentioned:

> My personal health information and intimacy details are exposed in public or private research app companies. I would be worried if my health personal information were misused or in the event of hacking instances, I would become a victim. (Texas, B)

When it comes to highly sensitive and risky data, users expect more security for app companies' data storage, preventing events such as hacking. However, as prior work noted, users' sensitive information stored in mHealth apps could be easily leaked through network traffic or log messages without being encrypted [56].

In addition to security practices, some participants (6/183, 3%) were concerned about app companies updating their data practices without notifying users. P7 reported:

> Their policy to share that data outside of the company could change and I would at the very least like to be informed about that and have the option to delete it. (Indiana, B)

Limited user control decreases trust toward period-tracking app companies' claimed practices. Users' control over their period-tracking apps' data (**User Control**) was the second most effective factor in explaining participants' level of privacy concerns with the apps. The regression results showed that compared to having no control, participants' privacy concerns' significantly dropped when being presented with an option to control their data (Table 3). Compared to data-sharing opt-out options, the data-deletion option was more effective in decreasing participants' privacy concerns (row 5: estimate = −2.52, p-value < 0.01).

Participants who expressed concerns about not having any type of control over their period-tracking apps' data reported that such lack of control would severely impact their trust toward the apps' companies and their claimed data practices (e.g., not sharing users' data with third parties). P36 mentioned:

> If you have no user control over your data, how do you know that it is being used ONLY as it says? (Wisconsin, B)

Consequently, for users like P36, having more data control means more insights into whether app companies' claimed policies match their practices. Therefore, we suggest increasing users' control to improve the data transparency of period-tracking apps, leading to more users' trust.

Participants were generally less concerned about apps that allowed data deletion. However, if apps shared data with healthcare providers or law enforcement, data deletion no longer reduced concern about the app, as indicated by the observed interaction effect (see rows 20, 21: estimates = 2.84, 1.75; p-values < 0.001, 0.05 respectively, Table 3).

Collecting location data is concerning as it is not relevant to apps' main functionality. Among the five tested levels of data type collected by period-tracking apps (**Collected Data**), participants perceived the collection of users' location to be most concerning (row 1: estimate = 1.72, p-value < 0.001). In their open-ended responses, participants most frequently (49/183, 27%) mentioned that the period-tracking apps' primary functionality should not rely on users' location and, therefore, such data collection is irrelevant and should not happen. This finding echoes an earlier finding regarding users' concern toward data sharing with unnecessary and irrelevant stakeholders such as law enforcement.

Intimacy and mental health data are perceived as highly personal and not required for period tracking. Our participants were significantly concerned about the collection of intimacy (row 2:

estimate = 1.66, p-value < 0.001) and mental health data (row 3: estimate = 0.839, p-value < 0.01). 26% of participants (47/183) found such information to be highly personal and were concerned about this data being accessed by others. P107 noted:

> Intimacy data is one of the most private parts of a person. There's always a potential mishap of leaked information. (New Jersey, L)

Lack of perceived relevancy to period tracking was again a commonly mentioned reason (12/47, 26%) as to why participants were significantly concerned about the collection of intimacy and mental health data. P110 said:

> For intimacy data, I don't feel that it is needed to have to track that. What about it is applicable to menstrual health? (Minnesota, L)

Least concerns toward the collection of menstrual data only. Compared to the tested levels of collected data, our participants perceived the lowest privacy concerns toward menstrual data to be collected by period-tracking apps, mainly due to its importance and relevancy for period tracking. P112 reported:

> The app's limited scope, focusing solely on menstrual cycle tracking, may lead users to believe that the data collected is used solely for the intended purpose without extensive profiling or analysis. (New Jersey, L)

By now, we have seen participants commonly against irrelevant and unnecessary data collection (location, intimacy, and mental health data) and sharing (with law enforcement). These findings suggest that users' concern toward period-tracking apps is closely tied to the relevance between data practices and main functionality (detailed in Section 5).

Political party and level of education show a significant association with perceived privacy concerns. Our results showed that women identifying as Republicans tended to be significantly more concerned about period-tracking apps' data practices compared to their Democratic counterparts (row 16: estimate = 1.11, p-value < 0.05). Half of participants who identified themselves as Republicans were living in states where abortion was banned. Such a higher level of concern toward period-tracking apps' privacy practices might be attributed to the legal landscape of their states.

In addition to participants' political party, there was a significant connection between the level of education and participants' reported privacy concerns toward period-tracking apps' data practices. Notably, compared to those having no degree, our participants who reported having a Bachelor's degree were significantly more concerned about period-tracking apps' data practices (row 13: estimate = 1.36, p-value < 0.01).

4.3 Privacy And Risk Mitigation Practices Toward Period-Tracking Apps (RQ1)

Usability and privacy concerns were the primary reasons to delete or switch period-tracking apps. We surfaced several reasons for why some participants (56/183, 31%) switched their period-tracking apps or stopped using them. The most common reasons (30/56, 54%) were the perceived lack of convenience and usability. P110 explained:

> I was using the Spot On period-tracking/birth control pill monitoring app by Planned Parenthood up until about 2018-2019. I initially stopped using it because it became high maintenance to remember to log my data every day. (Minnesota, L)

Following the poor usability, privacy concerns were the second most mentioned reason (12/59, 20%). Among them, 42% of responses (5/12) specified the overturn of Roe v. Wade as the main reason to stop using period-tracking apps or switch to a more privacy-protective app. P102 mentioned:

> I think there was one called Flo. I decided to stop using the apps and switched to Apple Health for tracking when Roe v. Wade was overturned. (Colorado, L)

Notably, looking at the fact that only 8% of all participants attributed their concern to the overturn of Roe v. Wade (Section 4.2), the proportion of participants who stopped using period-tracking apps due to the overturn was even lower (5/183, 3%). This may suggest that the overturn of Roe v. Wade has played a limited role in female users' privacy concerns and practices toward period-tracking apps.

Only a few participants took steps to mitigate their privacy concerns. Among our participants who expressed concerns toward period-tracking apps' data practices, only 9% (16/183) reported taking steps to manage their privacy concerns. Deleting the period-tracking apps was the most commonly used strategy to mitigate privacy concerns (6/16, 38%). Another practice that 31% of participants (5/16) mentioned was to seek information about the apps' data practices. P110 reported:

> I have taken the steps of reading an in-depth explanation of the app's security and sharing practices. In the example of the Spot On app, I read their privacy policy cover to cover and ensured that they would not share data. (Minnesota, L)

91% of our participants (167/183), however, mentioned that they had never used any mitigation strategies, mainly due to their lack of privacy knowledge and awareness. P127 mentioned:

> I have not yet done this as I was unsure how to proceed with this, and I did not know if these steps would be successful. (New Jersey, L)

13% of participants (2/16) reported that despite their concerns, they still had to use the app for health purposes. P11 said:

> I am not too concerned. I need to keep track of my cycles because I literally can't function on day 2 and 3. (Texas, B)

13% of participants (2/16), who lived in states where abortion was legal, reported that they felt safe and, therefore did not feel the need to take any further steps. P123 mentioned:

> I live in a state in which I feel safer about my reproductive health options; I do not feel scared that my data would impede my ability to get the care I need. (Minnesota, L)

In summary, echoing prior work [78], most participants did not do anything other than delete their apps. In addition, we found that for the majority of participants who did not have any mitigation

practices, feeling uninformed, dependence on the app functionality, and living in abortion-legal states were the primary reasons.

4.4 Privacy Attitudes And Awareness Toward The Overturn Of Roe v. Wade (RQ2)

We asked participants about their familiarity with the overturn of Roe v. Wade and its impact on their privacy perceptions and practices of period-tracking apps.

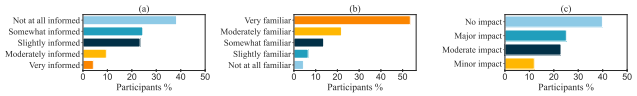

Figure 4: Participants' (a) knowledge level of the privacy practices of their PTA, (b) familiarity with the overturn of Roe v. Wade, and (c) perceived impact on concerns toward the privacy of their PTA post the overturn of Roe v. Wade.

Concerns toward potential privacy implications of the overturn of Roe v. Wade. Almost all participants reported to be at least slightly familiar with the overturn of Roe v. Wade. For 60% of participants (110/183), the overturn impacted their perceived concerns toward data practices of period-tracking apps (Figure 4). These participants expressed concerns about the potential consequences of period tracking. They suspected the data from period-tracking apps could be used to detect abortion and even criminalize users accordingly. 7% of those (8/110) mentioned in their open-ended responses that they had never thought about the potential privacy implications of the overturn before taking the survey, expressing appreciation to our study for raising their privacy awareness.

Our quantitative results showed that those who reported that the overturn impacted their privacy concerns indeed perceived significantly higher concerns (p-value < 0.05) toward data practices of the presented period-tracking app scenarios. 48% of those participants (53/110) predicted that the overturn would increase the chances for law enforcement to track individuals. P75 said:

> If they are tightening abortion laws and basically making it illegal (I live in the South), then they are going to start looking at our data. (Texas, B)

Among these participants, 17% of them (9/53) expected an increase in using period-tracking apps in case of need for abortions post the overturn. P9 mentioned:

> If access to safe and legal abortions becomes restricted or limited, individuals might rely more heavily on period-tracking apps to monitor their reproductive health. This could increase the amount of sensitive and personal health data shared with these apps. (Tennessee, B)

For 38% of participants (70/183) who perceived minimum or no privacy impact of the overturn of Roe v. Wade, they explained that they could not envision how the shared data would impact them in practice. P18 reported:

> I never thought that the overturn would cause law enforcement or healthcare providers to require app companies to share period-tracking data with them. But even if so, I'm not sure how it will impact the users since usually you just mark your starting date, mood, weight, etc. (Washington, L)

In summary, after participants were explicitly asked about the influence post the overturn of Roe v. Wade, most participants indicated their perceived huge influence. This may suggest that users' privacy concerns toward the overturn exist but have not yet been contextualized in their period-tracking app usage (detailed in Section 5.1).

4.5 Privacy Expectations Toward Period-Tracking Apps (RQ3)

We asked participants what privacy features they would like to have in period-tracking apps. In addition, we asked them who they believe is most responsible for protecting their period-tracking apps' data privacy and how.

4.5.1 Desired Privacy Features In Period-Tracking Apps: Usable Controls, Encryption, Granularity, And Anonymization. Collectively, our participants have expressed interest in features that can empower them with more data control, encryption, granularity, and anonymization. Among these features, more usable controls (e.g., data-deletion settings) were mentioned most (16/62, 26%). Having end-to-end encryption was the second most frequently requested feature (12/62, 19%). P24 mentioned:

> I wish there was an option to have the data be end-to-end encrypted so that not even the company knows the details of what I'm sharing with the app. (Texas, B)

For participants like P24, end-to-end encryption features would allow users to have more autonomy over their interactions with the apps. Having granular permission settings for data access was another feature our participants requested for more data control (9/62, 15%). P9 explained:

> Allowing users to customize permissions for different aspects of the app, like sharing data with other users or health professionals, could provide more control over their information (Tennessee, B).

From participants' qualitative responses, we can see different participants showed different receptivity to health professionals' having access to period-tracking data. They also had different perceptions of what types of information could be shared with health professionals. Therefore, a granular permission setting can help people with different privacy preferences better customize their choices, increasing users' autonomy over their data. In addition, 6% of participants (4/62) mentioned data anonymization as their desired privacy feature in period-tracking apps. These participants wanted their data to be anonymized before data collection and sharing.

4.5.2 Stakeholders Who Are Responsible To Protect Period-Tracking Apps' Data. In response to the multiple-choice questions regarding perceived stakeholders, 87% of participants (159/183) considered app developers to be most responsible for protecting their period-tracking apps' data privacy. Notably, participants' primary concern well aligns with what has been suggested in prior work [106] –

developers perceive reproductive data as "simply another piece of data rather than health data that is sensitive in nature" [106]. In addition, 49% of participants (90/183) perceived users as most responsible for protecting their own privacy. 48% (87/183) indicated mobile app store companies (e.g., Apple, Google) to be responsible, and 18% (33/183) attributed the responsibility to the government.

Call for app companies to improve the transparency of their privacy and security practices. In qualitative responses, participants who perceived the period-tracking app companies to be most responsible (146/183, 80%) requested the companies to 1) let users have more control over data deletion and sharing (80/183, 44%), 2) make privacy policies and user agreements transparent, simple, and straightforward (49/183, 27%), and 3) make sure the data is safe from law enforcement (11/183, 6%).

In particular, participants who expected more transparency (36/146, 25%) reported that they would most like to know about 1) the purposes of data usage (12/36, 33%), 2) whenever their data is being shared and with whom it is shared (12/36, 33%), 3) the benefits and risks of data sharing (7/36, 19%), 4) the types of controls that are available to users (3/36, 8%), 5) and the possibility of data recovery after deletion (2/36, 6%). For instance, P110 was interested in having easy access to information about data practices of period-tracking apps:

> I like to know if my data is being shared, and if so, where it is being shared. I'd also like to know how permanent my data is—as in, if I delete it, will it be permanently deleted or can it be recovered via some sort of hard drive of data kept by the app developer? (Minnesota, L)

P110's response covered many types of data transparency that are currently largely unavailable to users of period-tracking apps [4, 117]. For participants, data transparency is particularly important in the current political climate in the US. Hence, it is worth noting that eleven participants explicitly requested data safety from law enforcement. In better protecting users' reproductive privacy from law enforcement, we propose technology-based recommendations in Section 5.

Call for enhancing privacy law regulations. Participants (37/183, 20%) requested law sectors to enhance privacy regulations and protect users' data in period-tracking apps. P110 noted:

> I want to see a law passed that protects the privacy of all users of these apps AND their data. I also want to see that law upheld and not challenged by the courts. I think it is an infringement on our freedoms and privacy and should already be protected by amendments, but it isn't always. (Minnesota, L)

P110 emphasized law enforcement's role in ensuring their reproductive data can be unconditionally protected while acknowledging the reality, i.e., reproductive data is not always protected by amendments. Participants like P110 were correct, as reproductive data protections are poorly defined under several major legal frameworks in the US and beyond, e.g., HIPAA (US) [102], GDPR (EU) [79], MHRA (UK) [80]. In improving the effectiveness of law regulations for reproductive data, we propose policy-based recommendations in Section 5.

In summary, according to participants, there are many responsibilities to be fulfilled by app companies and law enforcement. Thus, a multi-stakeholder ecosystem must be established for more privacy support for female users of period-tracking apps, as their functionality still remains essential for some users (Section 4.3). In the next section, we will propose more actionable recommendations.

5 DISCUSSION

In brief, our findings highlight that among the tested data practices, the set of parties with whom the data is being shared was the most effective factor in impacting participants' privacy concerns toward period-tracking apps. More specifically, sharing with law enforcement was most concerning to participants (**RQ1**). Despite expressing significant concerns about the data practices of period-tracking apps, very few participants felt sufficiently empowered to take action beyond deleting the apps (**RQ1**). Our results showed that although most participants were familiar with the overturn of Roe v. Wade, they lacked sufficient awareness of how such an overturn might impact their reproductive privacy (**RQ2**). To protect their privacy, participants called for app companies and law enforcement to enhance their privacy practices and regulations (**RQ3**). In this section, we first discuss how our work extends the prior work in this area. With the key takeaways summarized, we then propose actionable recommendations grounded in our findings and related work.

5.1 (Re)contextualizing Women's Privacy Concerns Toward Period-Tracking Apps Post Roe v. Wade

Extensive prior work has discussed people's privacy perceptions and attitudes toward mHealth applications [45, 56, 88, 124], suggesting that people generally have concerns toward mHealth applications, especially when the applications collect sensitive health data [1, 80]. Building on this strand of work, our work has focused on women's privacy perceptions and attitudes toward their period-tracking data. However, in contrast to prior work, we focused on whether and how the changing landscape around abortion laws in the US has changed women's privacy perceptions, attitudes, and practices.

Without being explicitly asked about the overturn of Roe v. Wade, only 8% of our participants reported becoming more concerned about the data practices of their period-tracking apps due to the overturn (Section 4.2). This suggests that the majority of participants were not aware of the privacy implications of the overturn for their period-tracking practices.

Before being reminded about the overturn of Roe v. Wade, our participants' privacy concerns and attitudes were similar to the prior work focused on non-US users of FemTech (e.g., period- and fertility-tracking apps) [1, 11, 58, 80]. For instance, a 2023 UK-based study [80] found that FemTech users expressed concerns toward data sharing and users were generally unaware of their legal rights and technological privacy-enhancing protections.

We observed similar trends in our participants' privacy attitudes and practices. However, compared to the UK, where abortion is generally legal within the first 24 weeks of pregnancy [2], women's reproductive rights in the US have constantly been worsening since

the overturn [119]. Even when being directly asked about the overturn of Roe v. Wade, about 40% of participants still reported that the overturn had no impact on their period-tracking practices (Section 4.4). 38% of participants mentioned that they could not imagine how period-tracking apps share their data with law enforcement (Section 4.4). However, we have already seen cases where abortion-seeking women had been prosecuted for their access history to an abortion-related website, evidenced by US law enforcement [128].

Our findings suggest that due to a lack of risk awareness in the post Roe v. Wade context, women may still compromise their reproductive privacy to use such technologies. We argue an imperative need to contextualize women's privacy concerns toward period-tracking apps post Roe v. Wade. To help improve women's privacy awareness in the context of the overturn, we further provide actionable recommendations in Section 5.3.

5.2 Defining "Necessary" Data Practices and Data Safety from Governments

One prominent finding in our study is that participants expressed great concerns toward data practices whenever they were "unnecessary" and "irrelevant" to period tracking. For example, in participants' qualitative responses, the collection and/or sharing of non-menstrual cycle data (location, mental health, and intimacy data) with other parties, including third parties and law enforcement, were largely concerning (Section 4.2). Similarly, in another FemTech privacy study, participants urged apps not to require irrelevant information when signing up, such as home addresses [80].

As prior work has pointed out, reproductive health data has not been explicitly covered or defined in many major legal frameworks worldwide [43, 79, 80, 102], including HIPAA (US) [102], GDPR (EU) [79], and MHRA (UK) [80]. Moreover, Mehrnezhad et al. [79] evaluated the privacy notices and tracking practices of 30 top fertility-tracking apps, suggesting that these apps' indifference to users' privacy in their policies and data practices has been poorly regulated or defined by GDPR.

In the US, policy-based efforts have been made since the overturn, but we argue that these efforts still entail further improvement in defining "necessary" data practices. Since the overturn of Roe v. Wade, some policies have been released, particularly in response to the reproductive privacy crisis, including the My Body, My Data (MBMD) Act in 2022 [29] and My Health, My Data (MHMD) Act in 2023 [113]. In response to the gap of period-tracking data not being covered by HIPAA, the MBMD Act [29] aimed to control the sharing and sale of reproductive health data to third parties "except as is strictly necessary to provide a product or service." However, there is no definition or any information regarding what exactly could be considered as "strictly necessary." Theoretically, an app could still argue the necessity of providing the data for governments if requested.

Hence, another imperative problem with this Act lies in its oversight of law enforcement as a potential data-sharing party. Considering the worsening landscape around abortion laws, participants in our study expressed concerns about data sharing with law enforcement (Section 4.4). As requested by our participants, period-tracking app companies should make sure their data is safe from law enforcement (Section 4.5.2). However, in this Act, we found no information on how app companies should handle users' data when law enforcement requests it. In response to this alarming gap, we further provide recommendations in Section 5.3.

5.3 Calling For Privacy-Enhancing Technologies, Policies, and Education

Having discussed the imperative need to recontextualize women's privacy awareness and define necessary data practices post the overturn of Roe v. Wade, we now provide more concrete directions for privacy-enhancing technologies, policies, and education.

Technologies: Increasing data transparency, user control, and protections from law enforcement. Participants in our study called for app companies to enhance data transparency, user control, and protections from law enforcement (Section 4.5.2). Prior work has shown concerning facts about the data transparency of mHealth and period-tracking apps [3, 79, 117], including missing privacy policies [3, 117] and privacy-related content in their policies [79]. Besides privacy policies, another existing data transparency mechanism is privacy nutrition labels, which draw from the physical metaphor of food nutrition labels to enhance people's privacy awareness [34, 36–38, 68]. Hence, our first recommendation is to enhance the data transparency of period-tracking apps by referencing existing mechanisms, as mentioned above. In particular, when using existing data transparency mechanisms for period-tracking apps, it is worth taking relevant legal frameworks into account, especially the newly-released MBMD and MBMH Acts as mentioned in Section 5.2. Avoiding ambiguity when demonstrating the regulations in the policy is critical [79], such as defining what would happen if law enforcement requests data.

Notably, participants in our study mentioned they had trust problems with period-tracking apps' policies because selling health data to third parties such as insurance companies was perceived as hugely profitable (Section 4.2). To enhance the credibility of data transparency mechanisms, we argue that more user control is needed.

Having more user control would also be beneficial for users with diverse privacy attitudes toward different data types and data-sharing parties (e.g., health professionals) (Section 4.5.2). Hence, we suggest adding user control settings with wide choices and high granularity. We also emphasize that app companies must go beyond simply offering more user control settings. They should prioritize making these settings accessible and straightforward. For example, it is recommended to avoid the pitfalls of the privacy communication game [20], a strategy where apps superficially enhance privacy controls but intentionally design them to be complex or unclear.

Considering the potential data request by law enforcement post Roe v. Wade, we also suggest companies make it clear how they plan to handle data requests by law enforcement. As mentioned by participants, they would like their data to be anonymized before data collection (Section 4.5.2). Therefore, in protecting users from potential prosecution, it is worth considering not requiring users to input any personally identifiable information when signing up. For instance, apps can offer the users an option to use pseudonyms or not require an account for usage at all.

Policies: More considerations for potential conflicts with law enforcement and anonymization. As we have seen from the newly-released MBMD Act [29], data protection from law enforcement has not been defined yet. In future policies regarding data privacy of period-tracking apps, we recommend three considerations. First, policies should clearly specify if law enforcement can request access to reproductive health data from companies. This is particularly critical considering some of our participants expressed a lack of concern toward the overturn of Roe v. Wade, primarily because they perceived it unrealistic for law enforcement officers to have access to their period-tracking data (Section 4.4). Additionally, if law enforcement is likely to have data access, companies should be required to inform users in advance.

Education: Enhancing public awareness through the press and K12 curriculum. Since the overturn of Roe v. Wade, the number of articles about the dangers of women's mHealth apps has risen [32]. However, as we have seen from our participants' responses (Section 4.2) and our discussion regarding the recontextualization of women's privacy concerns post the overturn of Roe v. Wade (Section 5.1), more education efforts might be needed from the press and schools. The press is responsible for educating the public about the consequences of any unwary use of period-tracking apps, such as prosecution [65, 128]. In addition, schools could consider incorporating period-tracking app usage post the overturn of Roe v. Wade into their sex education or menstrual-related curricula.

6 CONCLUSION

Period-tracking apps track and collect a wide range of highly sensitive data, including women's menstrual cycle, pregnancy, sex life, location data, etc. The privacy concerns of period-tracking apps have been aggravated since the overturn of Roe v. Wade, which took away the constitutional right to abortion and led to diverse abortion laws across different states in the US. Given the current context, it is crucial to understand women's privacy perceptions and practices toward period-tracking apps. Moreover, how much knowledge and awareness women have about the impact of the overturn on their reproductive privacy is also a critical question to investigate in support of reproductive justice. In this study, we conducted a vignette survey study with 183 female participants in the US, who were evenly distributed in abortion-allowed and banned states. Our findings suggest that participants generally lacked awareness and information about period-tracking apps' data practices in the post Roe v. Wade era, despite showing privacy concerns. To better raise women's reproductive privacy awareness and empower them with more privacy-enhancing actions, we provide several actionable recommendations for different stakeholders.

ACKNOWLEDGMENTS

This work was supported by the Orau Ralph E Powe Junior Faculty Award (383001603) and the Duke University Trinity College of Arts & Sciences Award (4517834). We thank the anonymous reviewers for their valuable feedback.

REFERENCES

[1] 2023. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/09/ico-to-review-period-and-fertility-tracking-apps/

[2] 2023. https://en.wikipedia.org/wiki/Abortion_in_the_United_Kingdom#Citations

[3] Davey Alba. 2015. An app for hacking fertility now also works for men. https://www.wired.com/2015/04/glow/

[4] Najd Alfawzan, Markus Christen, Giovanni Spitale, Nikola Biller-Andorno, et al. 2022. Privacy, data sharing, and data security policies of women's mhealth apps: scoping review and content analysis. *JMIR mHealth and uHealth* 10, 5 (2022), e33735.

[5] Teresa Almeida. 2015. Designing intimate wearables to promote preventative health care practices. In *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers*. 659–662.

[6] Teresa Almeida, Rob Comber, and Madeline Balaam. 2016. HCI and Intimate Care as an Agenda for Change in Women's Health. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 2599–2611.

[7] Teresa Almeida, Rob Comber, Patrick Olivier, and Madeline Balaam. 2014. Intimate care: exploring etextiles for teaching female pelvic fitness. In *Proceedings of the 2014 companion publication on Designing Interactive Systems*. 5–8.

[8] Teresa Almeida, Rob Comber, Gavin Wood, Dean Saraf, and Madeline Balaam. 2016. On looking at the vagina through labella. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 1810–1821.

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

[10] Priscilla Alvarez. 2019. House Judiciary Committee asks former ORR director to clarify testimony on pregnant minors. https://edition.cnn.com/2019/03/22/politics/scott-lloyd-pregnant-minors/index.html Accessed: 2023-07-18.

[11] Katrin Amelang. 2022. (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*. Springer, 297–321.

[12] Sini-Marja Ant-Wuorinen, Maria Knaapi, Heli Koskela, Emma Lindberg, Anni Lintula, and Linda Palenius. [n. d.]. "Your period starts in two days" Risks of period-tracking post Roe v. Wade. ([n. d.]).

[13] Christiane Atzmüller and Peter M Steiner. 2010. Experimental vignette studies in survey research. *Methodology* (2010).

[14] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. 4. americans' attitudes and experiences with privacy policies and laws. *Pew Research Center: Internet, Science & Tech* (2019).

[15] Madeline Balaam, Lone Koefoed Hansen, Catherine D'Ignazio, Emma Simpson, Teresa Almeida, Stacey Kuznetsov, Mike Catt, and Marie LJ Søndergaard. 2017. Hacking women's health. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 476–483.

[16] Jeffrey Bardzell and Shaowen Bardzell. 2011. Pleasure is your birthright: digitally enabled designer sex toys as a case of third-wave HCI. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. 257–266.

[17] Shaowen Bardzell. 2010. Feminist HCI: taking stock and outlining an agenda for design. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1301–1310.

[18] Jeremy Birnholtz, Irina Shklovski, Mark Handel, and Eran Toch. 2015. Let's talk about sex (Apps), CSCW. In *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing*. 283–288.

[19] Nicole J-M Blackman and John J Koval. 2000. Interval estimation for Cohen's kappa as a measure of agreement. *Statistics in medicine* 19, 5 (2000), 723–741.

[20] Joseph Bonneau and Sören Preibusch. 2010. The privacy jungle: On the market for data protection in social networks. In *Economics of information security and privacy*. Springer, 121–167.

[21] The Census Bureau. 2022. U.S. Census Bureau quickfacts: United States. https://www.census.gov/quickfacts/fact/table/US/PST045222

[22] The Census Bureau. 2023. Educational Attainment in the United States: 2022. https://www.census.gov/data/tables/2022/demo/educational-attainment/cps-detailed-tables.html

[23] Samantha T Campanella. 2022. Menstrual and Fertility Tracking Apps and the Post Roe v. Wade Era. (2022).

[24] Nadia Campo Woytuk, Marie Louise Juul Søndergaard, Marianela Ciolfi Felice, and Madeline Balaam. 2020. Touching and being in touch with the menstruating body. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–14.

[25] PEW RESEARCH CENTER. 2020. Persistent gender gap in partisanship; men are more likely than women to identify as independents. https://www.pewresearch.org/politics/2020/06/02/democratic-edge-in-party-identification-narrows-slightly/pp_2020-06-02_party-id_1-02/

[26] Karine Coen-Sanchez, Bassey Ebenso, Ieman Mona El-Mowafi, Maria Berghs, Dina Idriss-Wheeler, and Sanni Yaya. 2022. Repercussions of overturning Roe v. Wade for women across systems and beyond borders. , 5 pages.

[27] Federal Trade Commission. 2021. FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others. https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-

data-facebook-google
[28] Federal Trade Commission. 2023. Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order. https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc
[29] Congress. 2022. S.4434 - My Body, My Data Act of 2022. https://www.congress.gov/bill/117th-congress/senate-bill/4434/text
[30] Judith B Cornelius, Janet S St Lawrence, Jacquelyn C Howard, Deval Shah, Avinash Poka, Delilah McDonald, and Ann C White. 2012. Adolescents' perceptions of a mobile cell phone text messaging-enhanced intervention and development of a mobile cell phone-based HIV prevention intervention. *Journal for specialists in pediatric nursing: JSPN* 17, 1 (2012), 61.
[31] Joseph Cox. 2022. Data broker is selling location data of people who visit abortion clinics. https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood
[32] Zikan Dong, Liu Wang, Hao Xie, Guoai Xu, and Haoyu Wang. 2022. Privacy Analysis of Period Tracking Mobile Apps in the Post-Roe v. Wade Era. In *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*. 1–6.
[33] Anna Eaglin and Shaowen Bardzell. 2011. Sex toys and designing for sexual wellness. In *CHI'11 Extended Abstracts on Human Factors in Computing Systems*. 1837–1842.
[34] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 447–464.
[35] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. 2018. The influence of friends and experts on privacy decision making in IoT scenarios. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 1–26.
[36] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2021. An informative security and privacy "nutrition" label for internet of things devices. *IEEE Security & Privacy* 20, 2 (2021), 31–39.
[37] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2021. Which privacy and security attributes most impact consumers' risk perception and willingness to purchase IoT devices?. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 519–536.
[38] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.
[39] Pardis Emami-Naeini, Tiona Francisco, Tadayoshi Kohno, and Franziska Roesner. 2021. Understanding Privacy Attitudes and Concerns Towards Remote Communications During the {COVID-19} Pandemic. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 695–714.
[40] Kim VL England. 1994. Getting personal: Reflexivity, positionality, and feminist research. *The professional geographer* 46, 1 (1994), 80–89.
[41] Henrik Enquist and Konrad Tollmar. 2008. The memory stone: a personal ICT device in health care. In *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*. 103–112.
[42] Daniel A Epstein, Nicole B Lee, Jennifer H Kang, Elena Agapie, Jessica Schroeder, Laura R Pina, James Fogarty, Julie A Kientz, and Sean Munson. 2017. Examining menstrual tracking to inform the design of personal informatics tools. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 6876–6888.
[43] Anna Essén, Ariel D Stern, Christoffer Bjerre Haase, Josip Car, Felix Greaves, Dragana Paparova, Steven Vandeput, Rik Wehrens, and David W Bates. 2022. Health app policy: international comparison of nine countries' approaches. *NPJ digital medicine* 5, 1 (2022), 31.
[44] Eliza Fawcett. 2022. Georgia's 6-Week Abortion Ban Begins Immediately After Court Ruling. https://www.nytimes.com/2022/07/20/us/georgia-abortion-ban.html Accessed: 2023-07-18.
[45] Ana Ferreira, Joana Muchagata, Pedro Vieira-Marques, Diogo Abrantes, and Soraia Teles. 2021. Perceptions of Security and Privacy in mHealth. In *International Conference on Human-Computer Interaction*. Springer, 297–309.
[46] Elizabeth Fife and Juan Orjuela. 2012. The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management* 4 (2012), 11.
[47] Margaret Flemings, Shanzay Kazmi, Rachel Pak, and Orit Shaer. 2018. Crimson wave: Shedding light on menstrual health. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction*. 343–348.
[48] Center for Reproductive Rights. 2022. High Court of Kenya in Malindi Ruling in PAK and Salim Mohammed vs. the Attorney General and 3 others. https://reproductiverights.org/high-court-of-kenya-in-malindi-ruling-in-pak-and-salim-mohammed-vs-the-attorney-general-and-3-others/ Accessed: 2023-07-18.
[49] The Organisation for the Review of Care and Health Apps. 2022. Data Privacy Matters... Period. *ORCHA Report on the Data Security of Period Tracking Apps* (2022).
[50] Leah R Fowler, Charlotte Gillard, and Stephanie R Morain. 2020. Readability and accessibility of terms of service and privacy policies for menstruation-tracking smartphone applications. *Health promotion practice* 21, 5 (2020), 679–683.
[51] Gennie Gebhart and Daly Barnett. [n. d.]. Should You Really Delete Your Period Tracking App? *Electronic Frontier Foundation* ([n. d.]). https://www.eff.org/deeplinks/2022/06/should-you-really-delete-your-period-tracking-app
[52] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security* 77 (2018), 226–261.
[53] Michael Hammond. 2010. What is an affordance and can it help us understand the use of ICT in education? *Education and Information Technologies* 15 (2010), 205–217.
[54] Josie Hamper. 2022. A fertility app for two? Women's perspectives on sharing conceptive fertility work with male partners. *Culture, health & sexuality* 24, 12 (2022), 1713–1728.
[55] Drew Harwell. 2019. Is your pregnancy app sharing your intimate data with your boss? https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/
[56] Dongjing He, Muhammad Naveed, Carl A Gunter, and Klara Nahrstedt. 2014. Security concerns in Android mHealth apps. In *AMIA annual symposium proceedings*, Vol. 2014. American Medical Informatics Association, 645.
[57] Kashmir Hill. [n. d.]. Deleting Your Period Tracker Won't Protect You. *The New York Times* ([n. d.]). https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html
[58] Bryndl Hohmann-Marriott. 2021. Periods as powerful data: User understandings of menstrual app data and information. *New Media & Society* (2021), 14614448211040245.
[59] Alexis Hope, Catherine D'Ignazio, Josephine Hoy, Rebecca Michelson, Jennifer Roberts, Kate Krontiris, and Ethan Zuckerman. 2019. Hackathons as participatory design: iterating feminist utopias. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–14.
[60] Guttmacher Institute. 2022. 13 States have abortion trigger bans—here's what happens when Roe is overturned. Guttmacher Institute. http://www.guttmacher.org/article/2022/06/13-states-have-abortion-trigger-bans-heres-what-happens-when-roe-overturned Accessed: 2023-07-18.
[61] Minal Jain and Pradeep Yammiyavar. 2015. Game based learning tool seeking peer support for empowering adolescent girls in rural Assam. In *Proceedings of the 14th International Conference on Interaction Design and Children*. 275–278.
[62] Guillermina Jasso. 2006. Factorial survey methods for studying beliefs and judgments. *Sociological Methods & Research* 34, 3 (2006), 334–423.
[63] Gopinaath Kannabiran, Alex A Ahmed, Matthew Wood, Madeline Balaam, Theresa Jean Tanenbaum, Shaowen Bardzell, and Jeffrey Bardzell. 2018. Design for sexual wellbeing in HCI. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–7.
[64] Gopinaath Kannabiran, Shaowen Bardzell, and Jeffrey Bardzell. 2012. Designing (for) desire: a critical study of technosexuality in HCI. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design*. 655–664.
[65] Martin Kaste. [n. d.]. Nebraska cops used Facebook messages to investigate an alleged illegal abortion. *National Public Radio* ([n. d.]). https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion
[66] Katharine Kemp. 2023. Your Body, Our Data: Unfair and Unsafe Privacy Practices of Popular Fertility Apps. *Social Science Research Network* (2023).
[67] Os Keyes, Burren Peil, Rua M Williams, and Katta Spiel. 2020. Reimagining (women's) health: HCI, gender and essentialised embodiment. *ACM Transactions on Computer-Human Interaction (TOCHI)* 27, 4 (2020), 1–42.
[68] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. 2022. Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*. 508–520.
[69] Takayuki Kosaka, Hajime Misumi, Takuya Iwamoto, Robert Songer, and Junichi Akita. 2011. " Mommy Tummy" a pregnancy experience system simulating fetal movement. In *ACM SIGGRAPH 2011 Emerging Technologies*. 1–1.
[70] Neha Kumar and Richard J Anderson. 2015. Mobile phones for maternal health in rural India. In *Proceedings of the 33rd annual acm conference on human factors in computing systems*. 427–436.
[71] Lorenz Kustosch, Carlos Gañán, Mattis van't Schip, Michel van Eeten, and Simon Parkin. 2023. Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding {IoT} Manufacturers Legally Responsible. In *32nd USENIX Security Symposium (USENIX Security 23)*. 1487–1504.
[72] Leona Lassak, Hanna Püschel, Tobias Gostomzyk, and Markus Dürmuth. [n. d.]. Introducing Data Trustees: A Vignette-Based Study Approach to Get Users in the Loop. ([n. d.]).
[73] Johanna Levy. 2018. Of mobiles and menses: researching period tracking apps and issues of response-ability. *Studies on Home and Community Science* 11, 2 (2018), 108–115.

[74] Yvonna S Lincoln. 2005. Context, lived experience, and qualitative research. *Research in organizations: Foundations and methods of inquiry* (2005), 221–232.

[75] Deborah Lupton. 2020. Australian women's use of health and fitness apps and wearable devices: a feminist new materialism analysis. *Feminist Media Studies* 20, 7 (2020), 983–998.

[76] Kirsten Martin and Helen Nissenbaum. 2016. Measuring privacy: An empirical test using context to expose confounding variables. *Colum. Sci. & Tech. L. Rev.* 18 (2016), 176.

[77] Kirsten E Martin. 2012. Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics* 111 (2012), 519–539.

[78] Nora Mcdonald and Nazanin Andalibi. 2023. "I Did Watch 'The Handmaid's Tale'": Threat Modeling Privacy Post-Roe in the United States. *ACM Transactions on Computer-Human Interaction* (2023).

[79] Maryam Mehrnezhad and Teresa Almeida. 2021. Caring for intimate data in fertility technologies. In *Proceedings of the 2021 CHI conference on human factors in computing systems*. 1–11.

[80] Maryam Mehrnezhad and Teresa Almeida. 2023. " 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. *arXiv preprint arXiv:2306.05956* (2023).

[81] Lydia Michie, Madeline Balaam, John McCarthy, Timur Osadchiy, and Kellie Morrissey. 2018. From her story, to our story: Digital storytelling as public engagement around abortion rights advocacy in Ireland. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–15.

[82] Sorina Mihaila. 2023. Period tracking app Flo launches feature for male partners. https://www.femtechworld.co.uk/news/period-tracking-app-flo-launches-feature-for-male-partners/

[83] Mozilla. [n. d.]. In Post Roe v. Wade Era, Mozilla Labels 18 of 25 Popular Period and Pregnancy Tracking Tech With *Privacy Not Included Warning. *Mozilla* ([n. d.]). https://foundation.mozilla.org/en/blog/in-post-roe-v-wade-era-mozilla-labels-18-of-25-popular-period-and-pregnancy-tracking-tech-with-privacy-not-included-warning/

[84] Maryam Mustafa, Amna Batool, Beenish Fatima, Fareeda Nawaz, Kentaro Toyama, and Agha Ali Raza. 2020. Patriarchy, maternal health and spiritual healing: Designing maternal health interventions in Pakistan. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[85] Maryam Mustafa, Kimia Tuz Zaman, Tallal Ahmad, Amna Batool, Masitah Ghazali, and Nova Ahmed. 2021. Religion and Women's Intimate Health: Towards an Inclusive Approach to Healthcare. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–13.

[86] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an {IoT} world. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 399–412.

[87] Aaron Necaise, Tangila Islam Tanni, Aneka Williams, Yan Solihin, Apu Kapadia, and Mary Jean Amon. 2023. User Preferences for Interdependent Privacy Preservation Strategies in Social Media. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW2 (2023), 1–30.

[88] Leysan Nurgalieva, David O'Callaghan, and Gavin Doherty. 2020. Security and privacy of mHealth applications: a scoping review. *IEEE Access* 8 (2020), 104247–104268.

[89] Amy Olivero. 2022. Privacy and digital health data: The femtech challenge. https://iapp.org/news/a/privacy-and-digital-health-data-the-femtech-challenge/

[90] Carly Page. 2022. Supreme Court overturns Roe v. Wade: Should You Delete Your Period-tracking app? https://techcrunch.com/2022/05/05/roe-wade-privacy-period-tracking#

[91] Laura Parson. 2019. Considering positionality: The ethics of conducting research with marginalized groups. *Research methods for social justice and equity in education* (2019), 15–32.

[92] Tamara Peyton, Erika Poole, Madhu Reddy, Jennifer Kraschnewski, and Cynthia Chuang. 2014. " Every pregnancy is different" designing mHealth for the pregnancy ecology. In *Proceedings of the 2014 conference on Designing interactive systems*. 577–586.

[93] Kristen Poli. 2022. The most popular period-tracking apps, ranked by Data Privacy. https://www.wired.com/story/period-tracking-apps-flo-clue-stardust-ranked-data-privacy/

[94] Annu Sible Prabhakar, Nikki Newhouse, Emma Simpson, Christine Wanjiru Mburu, Nova Ahmed, and Yunan Chen. 2019. MatHealthXB: Designing across borders for global maternal health. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–4.

[95] Emilee Rader. 2023. Data Privacy and Pluralistic Ignorance. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 457–471.

[96] Rachel Rebouché. 2016. Abortion rights as human rights. *Social & Legal Studies* 25, 6 (2016), 765–782.

[97] John Newman &; Amy Ritchie and Nick Jones. 2023. Ovulation Tracking app premom will be barred from sharing health data for advertising under proposed FTC Order. https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc

[98] Catherine Roberts. 2022. These Period Tracker Apps Say They Put Privacy First. Here's What We Found. https://www.consumerreports.org/health/health-privacy/period-tracker-apps-privacy-a2278134145/

[99] Dorothy E Roberts. 1990. The future of reproductive choice for poor women and women of color. *Women's Rts. L. Rep.* 12 (1990), 59.

[100] Luc Rocher, Julien M Hendrickx, and Yves-Alexandre De Montjoye. 2019. Estimating the success of re-identifications in incomplete datasets using generative models. *Nature communications* 10, 1 (2019), 1–9.

[101] David Roedl, Shaowen Bardzell, and Jeffrey Bardzell. 2015. Sustainable making? Balancing optimism and criticism in HCI discourse. *ACM Transactions on Computer-Human Interaction (TOCHI)* 22, 3 (2015), 1–27.

[102] Donna Rosato. [n. d.]. What your period tracker app knows about you. *Consumer Reports* ([n. d.]). https://www.consumerreports.org/health/health-privacy/what-your-period-tracker-app-knows-about-you-a8701683935/

[103] Johnny Saldaña. 2021. *The coding manual for qualitative researchers*. sage.

[104] Shruti Sannon and Andrea Forte. 2022. Privacy research with marginalized groups: what we know, what's needed, and what's next. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–33.

[105] Natalia Serenko. 2014. Informational, physical, and psychological privacy as determinants of patient behaviour in health care. In *Handbook of Research on Patient Safety and Quality Care through Health Informatics*. IGI Global, 1–20.

[106] Laura Shipp and Jorge Blasco. 2020. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proc. Priv. Enhancing Technol.* 2020, 4 (2020), 491–510.

[107] Tierney Sneed. 2022. Some states move quickly to ban abortion after Supreme Court ruling. https://www.cnn.com/2022/06/24/politics/abortion-ban-states-move-quickly/index.html Accessed: 2023-07-18.

[108] Marie Louise Juul Søndergaard. 2017. Intimate Design: Designing Intimacy As a Critical-Feminist Practice. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 320–325.

[109] Marie Louise Juul Søndergaard, Marianela Ciolfi Felice, and Madeline Balaam. 2021. Designing menstrual technologies with adolescents. In *Proceedings of the 2021 chi conference on human factors in computing systems*. 1–14.

[110] Marie Louise Juul Søndergaard and Lone Koefoed Hansen. 2016. PeriodShare: A bloody design fiction. In *Proceedings of the 9th Nordic Conference on Human-Computer Interaction*. 1–6.

[111] Statista. 2022. Leading period tracker and female health apps worldwide in April 2022, by downloads. https://www.statista.com/statistics/1307702/top-period-tracker-apps-worldwide-by-downloads/

[112] Statista. 2023. Contraception & Fertility Apps. https://www.statista.com/outlook/dmo/digital-health/ehealth/ehealth-apps/contraception-fertility-apps/worldwide

[113] David Stauss. 2023. Washington Legislature Passes My Health My Data Act. https://www.bytebacklaw.com/2023/04/washington-legislature-passes-my-health-my-data-act/

[114] Amanda Jean Stevenson. 2021. The pregnancy-related mortality impact of a total abortion ban in the United States: a research note on increased deaths due to remaining pregnant. *Demography* 58, 6 (2021), 2019–2028.

[115] Elizabeth Stowell, Mercedes C Lyson, Herman Saksono, Reneé C Wurth, Holly Jimison, Misha Pavel, and Andrea G Parker. 2018. Designing and evaluating mHealth interventions for vulnerable populations: A systematic review. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–17.

[116] Nina Sun et al. 2022. Overturning Roe v Wade: reproducing injustice.

[117] Gioacchino Tangari, Muhammad Ikram, Kiran Ijaz, Mohamed Ali Kaafar, and Shlomo Berkovsky. 2021. Mobile health and privacy: cross sectional study. *bmj* 373 (2021).

[118] Kaitlyn Tiffany. 2018. Period-tracking apps are not for women. https://www.vox.com/the-goods/2018/11/13/18079458/menstrual-tracking-surveillance-glow-clue-apple-health

[119] The New York Times. 2023. Tracking the States Where Abortion Is Banned. https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html?auth=login-google1tap&login=google1tap Accessed: 2023-07-18.

[120] Rina Torchinsky. 2022. How period tracking apps and data privacy fit into a post-Roe v. wade climate. https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps

[121] Bonnie Tran and Lee Na Choi. 2018. Menstrual maze: A toy exploring public engagement in menstrual health education. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–6.

[122] Anupriya Tuli, Shaan Chopra, Neha Kumar, and Pushpendra Singh. 2018. Learning from and with menstrupedia: Towards menstrual health education in India. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20.

[123] Anupriya Tuli, Shruti Dalvi, Neha Kumar, and Pushpendra Singh. 2019. "It'sa girl thing" Examining Challenges and Opportunities around Menstrual Health Education in India. *ACM Transactions on Computer-Human Interaction (TOCHI)* 26, 5 (2019), 1–24.

[124] Luisa Vervier, André Calero Valdez, and Martina Ziefle. 2019. " Attitude"-mHealth Apps and Users' Insights: An Empirical Approach to Understand the Antecedents of Attitudes towards mHealth Applications.. In *ICT4AWE*. 213–221.

[125] Niklas von Kalckreuth and Markus A Feufel. 2023. Extending the Privacy Calculus to the mHealth Domain: Survey Study on the Intention to Use mHealth Apps in Germany. *JMIR Human Factors* 10 (2023), e45503.

[126] Lisa Wallander. 2009. 25 years of factorial surveys in sociology: A review. *Social science research* 38, 3 (2009), 505–520.

[127] Zixin Wang, Danny Yuxing Huang, and Yaxing Yao. 2023. Exploring Tenants' Preferences of Privacy Negotiation in Airbnb. In *32nd USENIX Security Symposium (USENIX Security 23)*. 535–551.

[128] Cat Zakrzewski, Pranshu Verma, and Claire Parker. [n. d.]. Texts, web searches about abortion have been used to prosecute women. *The Washington Post* ([n. d.]). https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution

[129] Mengxi Zhu, Chuanhui Wu, Shijing Huang, Kai Zheng, Sean D Young, Xianglin Yan, and Qinjian Yuan. 2021. Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. *Telematics and Informatics* 61 (2021), 101601.

A SURVEY QUESTIONS

A.1 Consent Questions

We started the survey with a consent form and asked participants questions to obtain their consent to participate in the survey:

(1) I am 18 years or older.
- Yes
- No

(2) I have read and I understand the information above.
- Yes
- No

(3) I want to participate in this survey and continue with the task.
- Yes
- No

We presented four randomly selected scenarios to each participant. We asked the same follow-up questions at the end of each scenario. Here, we only include one scenario and its follow-up questions.

A.2 Scenario Questions (SQ)

> Imagine you are looking for a **period-tracking** app to install on your **phone** to **keep track of your menstrual cycle**. You see a period-tracking app with the following **data practices**: The app **only** collects your **menstrual cycle data** (e.g., days bleeding). This app will **store** your data on the **device**. Your data **will not be shared** with anyone. You have **the option to delete your data**.

(1) How concerned are you about the data practices of this period-tracking app?
- Not concerned
- Slightly concerned
- Somewhat concerned
- Moderately concerned
- Very concerned

If "Not concerned":

(1) Please explain why you are not at all concerned about the data practices of this period-tracking app.

If "Slightly concerned, Somewhat concerned, Moderately concerned, Very concerned":

(1) Please explain what data practices of this period-tracking app you are concerned about.

A.3 Attention-Check Question Example

(1) Where is the collected data being stored in the described period-tracking app?
- Device
- None

A.4 Usage of Period Tracking

(1) Have you ever used any tool or method to track your period?
- Yes
- No

If "Yes" is selected:

- Please specify what methods you have used. (select all that apply)
  - period-tracking app on my phone
  - period-tracking app on my personal computer or tablet
  - period-tracking app on my wearable device
  - Paper diary/calendar/planner
  - Digital diary/calendar/planner
  - Using birth control pills

  If (period-tracking app on my phone, period-tracking app on my personal computer or tablet, period-tracking app on my wearable device) is selected:
  - Please specify what period-tracking app(s) you are currently using. (select all that apply): We provided a list of most frequently downloaded period-tracking apps (e.g., MyFLO, Drip), where participants can select from. In addition to the apps, we added two options: *I am not currently using any period-tracking app* and *Other (please specify)*.
  - For what purposes do you mainly use or have you used, your period-tracking app? (select all that apply)
    - Becoming aware of how my body is doing
    - Understanding my body's reactions to different phases of my menstrual cycle
    - To become prepared for the upcoming periods
    - To track fertility and plan (not) to get pregnant
    - To inform conversations with my healthcare providers
    - Other (please specify)
  - Have you ever had any period-tracking app that you stopped using after a while?
    - Yes
    - No

    If 'Yes' is selected for the previous question:
    - Please explain what period-tracking app(s) you stopped using and the reasons why you decided not to use these period-tracking app(s).

For all participants

- Please specify how likely you are to download a period-tracking app if recommended by the following groups/individuals:
  - Groups/individuals are:
    - My friend(s)
    - My family member(s)
    - My employer(s)
    - My insurance company
    - The government and law enforcement officers
    - Healthcare professionals (e.g., OB-GYN)
    - Romantic partner(s)
    - Privacy experts
    - App reviews
  - Choices are:
    - Not at all likely
    - Not so likely
    - Somewhat likely
    - Very likely
    - Extremely likely

A.5 Concerns Toward Period Tracking

If (period-tracking app on my phone, period-tracking app on my personal computer or tablet, period-tracking app on my wearable device) is selected:

- How concerned are you about the data practices of your period-tracking apps?
  - Not concerned
  - Slightly concerned
  - Somewhat concerned
  - Moderately concerned
  - Very concerned

  If (Slightly concerned, Somewhat concerned, Moderately concerned, Very concerned) is selected:
  - Have you ever taken any steps to mitigate your concerns about your period-tracking apps?
    - Yes
    - No

    If "Yes" is selected:
    - Please explain what steps you have taken to mitigate your concerns about your period-tracking apps.

    If "No" is selected:
    - Please explain why you have not taken any steps to mitigate your concerns about your period-tracking apps.
- Please specify if there are any security or privacy protections or features you wish were offered by your period-tracking apps.

For all participants

- Please rate your level of concern about the privacy implications of the following period and fertility tracking practices:
  - Period and fertility tracking practices:
    - Using a paper diary/calendar/planner to track my menstrual cycles
    - Using a digital diary/calendar/planner (e.g., Google Calendar) to track my menstrual cycles
    - Using a period-tracking app on my phone to track my menstrual cycles
    - Using a period-tracking app on my personal computer or tablet to track my menstrual cycles
    - Using a period-tracking app on my wearable device (e.g., smartwatch, smart ring) to track my menstrual cycles
    - Searching online about period and fertility-related topics
    - Posting online on social media about period and fertility-related topics
    - Using communication tools (e.g., WhatsApp, Telegram) to discuss period and fertility-related topics with others
  - Choices for concern level:
    - Not at all concerned
    - Not so concerned
    - Somewhat concerned
    - Very concerned
    - Extremely concerned
- Who do you think is most responsible for protecting the privacy of period tracking data?
  - The developers of the apps
  - The government
  - The users of period-tracking apps
  - Other (please specify)
- Please specify what specific actions do you want these responsible individuals/groups to take to protect the privacy of period tracking data

A.6 Information Toward Data Practices of Period-Tracking Apps

If (period-tracking app on my phone, period-tracking app on my personal computer or tablet, period-tracking app on my wearable device) is selected:

- How informed are you about the data practices of your period-tracking apps?
  - Not at all informed
  - Slightly informed
  - Somewhat informed
  - Moderately informed
  - Very informed

  If (Slightly informed, Somewhat informed, Moderately informed, Very informed) is selected:
  - Please explain what resources you usually use to become informed about the data practices of your period-tracking apps.
- Please explain what information about the privacy and data practices of your period-tracking apps you would like to know about, if any.

A.7 Knowledge and Concerns Toward the Overturn of Roe v Wade Decision

- How familiar are you with the overturn of the Roe v. Wade case/decision?
  - Not at all informed
  - Slightly informed
  - Somewhat informed
  - Moderately informed
  - Very informed
- In your own words, how would you describe the (overturn of) Roe v. Wade case/decision?
- How much impact do you think the overturn of Roe v. Wade has had on your concerns about the data practices of period-tracking apps?
  - No impact
  - Minor impact
  - Moderate impact
  - Major impact

  If Minor impact, Moderate impact, Major impact is selected
  - Please explain how the overturn of Roe v. Wade has impacted your concerns about the data practices of period-tracking apps.

  Else
  - Please explain why the overturn of Roe v. Wade had no impact on your concerns about the data practices of period-tracking apps.
- Have you ever applied any changes to your period tracking habits due to the overturn of Roe v. Wade?

  - Yes
  - No

  If "Yes" is selected
  - Please explain what changes you have applied to your period tracking habits due to the overturn of Roe v. Wade.

  If "No" is selected
  - Please explain why you have not applied any changes to your period tracking habits due to the overturn of Roe v. Wade.

A.8 Demographics

- What is your age? Please leave this question blank if you are not comfortable sharing your age.
- How do you describe your current gender identity?
  - Cisgender Female
  - Cisgender Male
  - Transgender Female
  - Transgender Male
  - Non-binary
  - Prefer to self-describe (please specify)
  - Prefer not to say
- Do you identify as a member of the LGBTQ* Community?
  - Yes
  - Maybe
  - No
  - Prefer not to say
- How do you describe your race or ethnic identity? (select all that apply)
  - American Indian or Alaskan Native
  - Asian
  - Black or African American
  - Hispanic or Latino, or Spanish Origin of any race
  - Native Hawaiian or Other Pacific Islander
  - White
  - Prefer not to say
  - Other (please specify)
- What is the highest degree you have earned?
  - No schooling completed
  - Nursery school
  - Grades 1 through 11
  - 12th grade—no diploma
  - Regular high school diploma
  - GED or alternative credential
  - Some college credit, but less than 1 year of college
  - 1 or more years of college credit, no degree
  - Associate's degree (for example: AA, AS)
  - Bachelor's degree (for example: BA. BS)
  - Master's degree (for example: MA, MS, MEng, MEd, MSW, MBA)
  - Professional degree beyond bachelor's degree (for example: MD, DDS, DVM, LLB, JD)
  - Doctorate degree (for example, PhD, EdD)
  - Prefer not to say
- What is your current marital status?
  - Single
  - Married
  - Divorced
  - Bereaved
  - Other (please specify)
  - Prefer not to say
- Which of these best describes the general area where you live?
  - Urban
  - Suburban
  - Rural
  - Other (please specify)
  - Prefer not to say
  - I do not know
- In which state do you currently reside? (50 states)
- In general, what is your political affiliation?
  - Democrat
  - Republican
  - Independent
  - Other (please specify)
  - None
  - Prefer not to say

B QUALITATIVE CODEBOOK

The codebook is available at:
https://osf.io/y7aud/?view_only=fc7469d974b54711ae970cdeb68eab92.

C FULL DEMOGRAPHIC INFORMATION

Age		State		Race		Political Affiliation		Degree		Marital Status		Area		Sexual Orientation	
Mean	39.05	Legal abortion state	51.37%	White	73.8%	Democrat	52.5%	Bachelor's degree	33.3%	Married	39.9%	Suburban	52.5%	Non-LGBTQ	67.8%
Range	19-75	Full abortion ban state	47.54%	Black or African American	4.9%	Independent	21.8%	1 or more years of college credit, no degree	15.3%	Single	36.1%	Urban	25.7%	LGBTQ	25.1%
STD	12.34	Prefer not to say	1.09%	Asian	3.3%	Republican	17.5%	Associate's degree	12.0%	Divorced	15.3%	Rural	19.7%	Maybe-LGBTQ	5.5%
				Hispanic or Latino, or Spanish Origin of any race	2.7%	None	3.8%	Some college credit, but less than 1 year of college	11.5%	Bereaved	4.3%	Prefer not to say	1.6%	Prefer not to say	1.6%
				American Indian or Alaskan Native	1.6%	Other*	2.2%	Regular high school diploma	10.4%	Other	3.3%	Other	0.5%		
				Prefer not to say	1.1%	Prefer not say	2.2%	Master's degree	9.3%	Prefer not to say	1.1%				
				Multiracial	12.6%			GED or alternative credential	2.7%						
								Doctorate degree	2.7%						
								Professional degree beyond bachelor's degree	1.1%						
								Prefer not to say	1.1%						
								12th grade—no diploma	0.6%						

Table 4: Complete demographic information of our participants.