"Users are worried, but we are confused": Exploring the Privacy, Security, and Safety Perspectives and Practices of FemHealth App Product Team Members

Chenkai Ma*
King's College London
chenkai.ma@kcl.ac.uk

Shijing He*
King's College London
shijing.he@kcl.ac.uk

Ina Kaleva
King's College London
ina.1.kaleva@kcl.ac.uk

Alisa Frik
International Computer Science Institute
afrik@icsi.berkeley.edu

Jose Such
INGENIO (CSIC-Universitat Politècnica de València)
jose.such@csic.es

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

Abstract

FemHealth apps (e.g., period, fertility, and pregnancy trackers) collect highly sensitive sexual and reproductive health data and have become a focal point for privacy, security, and safety (PSS) concerns, particularly amid changes in reproductive health regulations in the US and growing public scrutiny. While prior work has identified shortcomings in the PSS protections implemented by FemHealth apps, far less is known about how the *product teams* developing these apps conceptualize and operationalize PSS in practice. We conducted semi-structured interviews with 14 FemHealth app product team members who represented 11 unique apps and held diverse roles, including software engineering and architecture, security and privacy, product management, policy and legal compliance, and UX/UI research and design. We found that data collection decisions are often driven by feature-specific objectives, such as improving prediction accuracy and enabling reliable backups, rather than by explicitly articulated PSS requirements. Teams also frequently rely on legal compliance frameworks and PSS practices designed for general-purpose apps, while expressing confidence that these measures provide adequate protection. In addition, we identified four persistent challenges faced by FemHealth app product teams: disagreement over whether FemHealth apps require distinct PSS protections compared to non-FemHealth apps; difficulty establishing and maintaining user trust; uncertainty arising from cross-border enforcement related to abortion; and technical limitations associated with backups, end-to-end encryption, and coercive local access to data. Based on these findings, we derive a set of requirements and provide actionable technical and policy recommendations to inform the design, engineering, and governance of PSS in FemHealth apps.

Keywords

Mobile health (mHealth) apps, FemTech, privacy engineering, software development

*Both authors contributed equally to this research.

Proceedings on Privacy Enhancing Technologies 2026(4), 852–868

https://doi.org/10.56553/popets-2026-0148

1 Introduction

The global FemHealth app[1] market is rapidly growing and was valued at USD 4.85 billion in 2024, with the US accounting for the largest share [146]. These apps often collect and process user data to track menstrual cycles, fertility, pregnancy, and other aspects of sexual and reproductive health. Some also provide convenient and cost-effective healthcare information and advice, such as predictions of fertility-related diseases [90, 125]. Many of these apps generate inferences about users' health and app usage; however, such inferences often lack explicit legal protections for users' personally identifiable information (PII) and are not communicated transparently to users [111]. Although some users are aware of the *privacy, security, and safety (PSS)* risks and potential harms associated with using these apps (e.g., being prosecuted for a possible abortion based on data entered into the apps) [116], many struggle to understand how to effectively manage these risks and protect themselves from PSS harms [119] (see §2.2). In addition to authorities seeking access to users' data [74, 116], FemHealth app users may face threats from other actors, including insurers [143], conservative and religious individuals or groups with stigmatizing beliefs [2, 3, 84, 187], and abusive intimate partners [52, 148, 192].

Despite increasing attention in research and public discourse to PSS concerns surrounding FemHealth apps and FemTech more broadly, particularly following the U.S. Supreme Court's Dobbs v. Jackson Women's Health Organization decision, which removed federal protection for abortion rights [88], most existing work has focused on end users [38, 90, 116, 119, 135], or on analyzing app behaviors (e.g., via dynamic analysis) and policy artifacts (e.g., privacy policies) [10, 56, 99, 111]. Comparatively little attention has been paid to the PSS perspectives and practices of **product team members** involved in the design, development, and maintenance of FemHealth apps (see §2.2 and §2.3). Following prior work [73], we define "product team members" as individuals who contribute to the design, development, or maintenance of FemHealth apps. Given their influence over app functionality and data-handling practices, understanding their perspectives is critical. To address this gap, we investigate the following research questions (RQs):

[1]In this paper, we use the term "FemHealth apps" for simplicity and consistency with how these technologies are referred to in the FemTech industry. However, we understand that this term may not fully represent the diversity of FemHealth app users, as these apps can be used by people of any sex or gender assigned at birth.

RQ1: What are the PSS perspectives and practices of FemHealth app product team members?

RQ2: What PSS challenges do FemHealth app product team members face?

To answer our RQs, we conducted semi-structured interviews with 14 FemHealth app product team members from diverse backgrounds and demographics, varying in gender, location, age, educational attainment, professional experience, and team size. Our participants represented 11 unique apps. During the interviews, we explored participants' views on their FemHealth apps' data practices, PSS concerns and the strategies used to address them, available PSS resources and support for product teams, and legal and regulatory considerations.

Contributions. Our work makes three main contributions. First, we provide rich qualitative evidence of how FemHealth app product team members reason about data collection and implement PSS protections during design and development, complementing prior audits and policy analyses that primarily infer practices from in-app user interface features and privacy policies. Second, we identify four recurring PSS challenges that shape FemHealth app design and engineering in practice: (i) contested views on whether FemHealth apps are "unique" from a PSS perspective, (ii) difficulties in earning and maintaining user trust amid political change and social media amplification, (iii) uncertainty arising from tensions between data protection obligations and abortion-restriction enforcement pressures, and (iv) technical constraints related to backups, account recovery, and end-to-end encryption (E2EE), particularly in the presence of coercive threat actors. Third, we translate our findings into concrete PSS requirements and offer actionable recommendations for FemHealth app product teams and policymakers.

2 Related Work

2.1 PSS in Mobile Health (mHealth) Apps

Users are increasingly turning to digital tools to better understand [67, 134] and manage their health [22, 41], with mobile health (mHealth) apps widely used for tracking and managing both general health and specific medical conditions. However, a range of security and privacy threats [138], along with transparency issues [57, 80], have been identified in mHealth apps, raising user concerns [140]. These issues can create safety risks, particularly given the sensitivity of the data handled by such apps [37, 132, 193]. As a result, mHealth apps must establish and maintain high levels of user trust to support sustained adoption and long-term use [171]. Notably, perceptions of privacy and safety in mHealth apps are highly contextual, with both the type of app and the nature of the data collected significantly shaping users' attitudes [21].

2.2 PSS in FemHealth Apps

In addition to the PSS risks common to all mHealth apps, FemHealth apps–a specialized category of mHealth apps–introduce a distinct set of PSS risks due to the nature of the data they collect and the potential threat actors involved. These apps primarily collect and process highly sensitive personal health data, including sexual and reproductive health information [78, 81, 144]. Many also collect behavioral and location data, sometimes without users' explicit consent [10], thereby further increasing PSS risks [120]. While FemHealth apps frequently share personal data with third parties [56, 105], responsibility for managing these risks is often shifted onto users [111], and app privacy policies are frequently insufficiently transparent [61, 154]. These risks are further amplified by the stigma associated with certain reproductive health conditions, such as unintended pregnancy [163], abortion [20, 110], miscarriage [36], and infertility [136, 203].

FemHealth app users also vary in how they perceive and respond to these risks. Some report positive experiences with FemHealth apps [49], while others, aware of the sensitivity of their data [170], describe limited understanding of, and control over, data practices [79]. These users are often forced to choose between not using the app or accepting all terms and conditions [102, 118], leading to feelings of powerlessness [38]. At the same time, some users turn to social media to collectively discuss and address their concerns [169].

Abortion rights vary widely across countries and U.S. states, and in restrictive settings, FemHealth app data can be weaponized to surveil, criminalize, or prosecute users. In the U.S., abortion access restrictions began after Texas Senate Bill 8 (September 2021) [184]. On June 24, 2022, the Supreme Court's Dobbs v. Jackson Women's Health Organization decision overturned Roe v. Wade (1973) [86] and Planned Parenthood v. Casey (1992) [87], removing federal constitutional protection for abortion [88]. Since then, some state policies have further restricted access to abortion [26, 109, 166, 173, 186], sometimes leading to preventable harms, such as increased infant mortality rates [66]. In England and Wales, abortion access has also been constrained by legal and procedural conditions [107, 108, 185], alongside strengthening political voices opposing abortion rights [30, 47, 114, 174] and enforcement actions related to abortion [48, 59, 188]. Meanwhile, protections of abortion rights remain limited in some other jurisdictions, including parts of the EU [117] and El Salvador [165, 191].

The Roe v. Wade decision by the U.S. Supreme Court in 1973 often served as a reference point for strengthening abortion rights around the globe [91]. The Dobbs decision, which overturned Roe v. Wade, amplified ideas popular in the global anti-abortion coalition, which favor jurisdiction-based considerations of abortion rights over federal or multilateral agreements [123]. Such changes in the U.S. can encourage global actions protecting abortion rights on the one hand [91], and a global wave of anti-abortion actions on the other hand [4, 91]. Thus, following the Dobbs decision, FemHealth app users worldwide have shifted from being often indifferent to PSS risks [16, 34] to expressing increased concerns [111, 119, 125]. Seemingly benign FemHealth data (e.g., menstrual dates and heart rate) can be used to infer highly sensitive health information, including pregnancy and abortion status [15, 95]. Additional concerns have been raised about IP addresses that enable user tracking and the collection of data for advertising purposes [198]. Despite reassurances from product teams [168], many FemHealth apps have been found to suffer from security vulnerabilities [150]. However, despite a substantial body of research on FemHealth apps and their users, comparatively little attention has been paid to FemHealth app product teams that can improve apps or address user concerns, but that may also introduce PSS risks into their apps.

2.3 PSS in App Design and Development

PSS issues have been extensively studied across different stages of app design and development. Prior work has examined concerns such as unnecessary data collection [72, 176], unintended data leakage [63, 157, 194], extensive data-sharing practices [93], and limited user control over personal data [130]. Although users' perceptions of privacy are inherently subjective [195], they consistently express a desire for greater control over their data [13, 103], often pointing to the need for app-level improvements [28, 197]. Numerous design approaches have been proposed to improve user privacy and safety, including clearer privacy policies [145, 200], AI-powered methods to better inform users [196], and nudges that encourage better PSS-related decisions [43, 113, 202]. However, these approaches face several challenges, as users may perceive them as burdensome to use [25, 58, 71, 167] or as too costly or overwhelming to adopt in practice [164, 175]. As a result, effective PSS design must account for the interests of different stakeholders and remain sensitive to contextual factors [24, 111, 128].

While many studies have shown that it is not easy for product teams to build and maintain users' trust [137, 142, 160, 162], app product teams often de-prioritize PSS for various reasons, including revenue-driven incentives [53, 94, 98, 176, 182]. They also encounter technical challenges, such as deploying E2EE and secure cloud services [14, 50, 151, 183], and organizational barriers [1, 73, 92, 106, 131, 155, 180], such as problematic third-party services [44, 70] and a lack of actionable PSS guidance [98, 181]. In addition, product teams often struggle to interpret and implement PSS-related laws and regulations in practice [12, 179], as well as concerns regarding multi-jurisdictional compliance [141]. Although prior research has explored ways to support product teams in improving PSS, such as addressing code vulnerabilities [106], making more informed data-sharing decisions [177], complying with regulations [179], ensuring secure data transmission [68, 96], strengthening secure development and testing practices [5, 6, 39], and promoting secure AI use [62], product teams often rely primarily on app marketplace requirements and automated vulnerability checks [12, 182]. While research has introduced various methods to integrate PSS considerations into the software design and development process [82, 83, 161, 201], including Privacy by Design (PbD) principles and strategies [40, 45, 75, 76], few studies have taken the perspective of product teams or differentiated between responsibilities across different team roles [141]. Finally, because product teams developing FemHealth apps remain largely understudied, it is unclear whether they face distinct challenges and how they can best be supported.

2.4 Summary of Gaps in Prior Work

Prior work has examined PSS in FemHealth apps (§2.2) and in app design and development (§2.3). However, within the FemHealth app context, research has primarily focused on apps (e.g., analysis of privacy policies, network traffic, and UI/UX) and users, leaving the perspectives and practices of FemHealth app product teams largely understudied. Existing studies often infer data practices and risks from privacy policies or user comments. However, empirical evidence remains limited regarding how FemHealth app product teams reason about trade-offs, threat actors, and compliance obligations, particularly in a post-Dobbs environment. In this context, the same data may attract new and different threat actors and carry heightened legal risks compared to the period prior to the decision overturning Roe v. Wade.

Moreover, although the broader app security literature proposes many PSS strategies (e.g., data minimization, user controls, secure development, and improved disclosures), it remains unclear how these strategies are interpreted, prioritized, and operationalized by FemHealth app product teams under real technical and organizational constraints. Finally, despite FemHealth apps being widely characterized as a distinctive subcategory of mHealth, due to sensitive reproductive data and stigma-related harms, little is known about how product teams perceive this "uniqueness," and how it shapes their design and development decisions, governance practices, and assumptions about sufficient PSS protections.

3 Methodology

All supplementary materials, including the screening survey, interview guide, and codebook, are available in this OSF repository[2].

3.1 Participant Recruitment

We asked each potential participant to complete a screening survey to recruit a diverse sample of FemHealth app product team members, varying in mobile app design and development experience, product team size, team responsibilities, and educational background. Eligible participants were required to be 18 years or older, fluent or native English speakers, and to have been involved in the design and/or development of at least one mobile app that met all of the following criteria:

(1) The app tracks users' periods, fertility, pregnancy, or other aspects of sexual and reproductive health.
(2) The app is published on an app marketplace (e.g., Google Play Store or Apple App Store).
(3) The app collects user data to provide its services.
(4) The app is primarily designed for consumer use rather than exclusively for healthcare professionals.

We initially shared the screening survey link via social media platforms (LinkedIn, Facebook, and X) and Prolific. However, after identifying challenges in verifying participants' experience in developing FemHealth apps and ensuring data quality, we discontinued these recruitment channels. Consequently, we excluded all interview data from participants recruited through these platforms, as we observed substantial discrepancies between participants' self-reported expertise in the screening survey and their demonstrated knowledge and experience during interviews. We subsequently shifted to recruiting participants exclusively through direct emails obtained from publicly available sources (i.e., app marketplace listings and FemHealth app websites) and through direct messages on LinkedIn after reviewing corresponding profiles. The Research Ethics Committee of the primary author's institution approved the study, including the recruitment approach, following careful ethical review, as all contact information was publicly available and recruitment attempts were intentionally limited to avoid spamming.

[2] https://osf.io/3pkrz/?view_only=a8180e0dfd1d4942b1b14509e78afc25

In addition, we leveraged our professional networks and snowball sampling to recruit additional participants [133]. Of the 14 participants, seven were recruited via direct messages on LinkedIn, four through snowball sampling, and three via email.

Table 1 summarizes the aggregated characteristics of participants. We aggregated characteristics to prevent de-anonymizing participants and their companies or apps. Our sample reflects substantial diversity in gender, location of residence, age, educational background, tenure in app design and development, app availability regions, team size, and role responsibilities. Notably, only four participants held a single responsibility, while ten held multiple responsibilities. Participants from smaller product teams tended to combine more responsibilities, as also observed in other studies [12, 23]. We view the diversity of team responsibilities among our participants as a methodological strength. PbD and regulatory compliance are collaborative processes distributed across team members with diverse responsibilities [40, 45, 75, 76], whose complementary expertise and decisions shape not only legal risk assessments and technical safeguards, but also data transparency, user communication, and the design of user-centered data controls and security and privacy features. Including these perspectives enables a more holistic understanding of how real-world teams implement and interpret compliance and PSS requirements in practice.

Across the eleven unique FemHealth apps that our participants worked on[3], three were branded as menstruation apps, two as pregnancy apps, and six as both. However, all apps included calendar-based functionality, allowing users to record a wide range of personal information regardless of branding. Each participant was compensated £50 (or the equivalent in local currency) for an expected one-hour time commitment.

3.2 Interview Procedure

We conducted all semi-structured interviews remotely via Microsoft Teams[4], using the first author's institutional license. Interviews lasted an average of 64 minutes (min: 47 minutes; max: 81 minutes). When some interview questions remained at the end of the first hour, we offered participants the option to end the interview without penalty or continue; all participants chose to continue. Participants did not need a Microsoft Teams account to participate. All sessions were audio-recorded and transcribed using the same software. The first author then listened to each recording and manually verified the transcripts word by word to ensure accuracy. Our interview guide comprised seven main sections: warm-up, app practices, privacy risks and concerns, mitigation strategies, privacy communication mechanisms, resources, and regulations.

If participants had worked on multiple eligible apps, we asked them to select the app to which they had contributed the most as the main focus of the interview. When their contributions were comparable across apps, participants selected the app they had worked on or updated most recently. We also invited participants to share perspectives and experiences from their work on other FemHealth apps if these differed from those discussed for the main app; however, this occurred rarely.

[3] Although we contacted candidates representing more than 11 apps, not all responded or qualified. As a result, some participants represented the same app but held different responsibilities, providing diverse and sometimes complementary perspectives.
[4] https://www.microsoft.com/en-us/microsoft-teams/

Pilots. We conducted pilot interviews with four participants to refine the interview protocol and improve its conversational flow. Based on these pilots, we removed detailed questions about writing privacy statements (e.g., privacy policies), as many product team members were not directly involved in this process. We also observed that participants provided more nuanced responses when specific prompts followed their initial unaided recall. Accordingly, we introduced additional probes on privacy mitigation strategies, organizational barriers, and information sources. These probes were used only after participants' initial responses to minimize bias. Due to substantial revisions to the interview protocol, we excluded pilot interviews from the main dataset.

3.3 Research Ethics

To address ethical concerns, we employed several strategies. First, we obtained informed consent from all participants. Access to interview transcripts was restricted to the research team and stored and shared via the OneDrive cloud service provided by the first author's university. In addition, Microsoft Teams provided E2EE to support secure data handling [122]. Second, we removed all identifying details from quoted material to protect participants and the FemHealth apps they worked on from identification. The collected data could reveal sensitive information about apps' security postures, privacy practices, safety features, business strategies, technical architectures, and organizational structures, all of which warranted confidentiality. We also paraphrased all quotes, as explicitly requested by two participants, to avoid identification through wording similar to their apps' advertising phrases. Finally, we assigned random participant pseudonyms (P1–P14).

3.4 Data Analysis

The first two authors conducted reflective thematic analysis [32] using a *small q* approach [29, 31]. They began by independently coding two randomly selected transcripts, each developing an initial codebook. The authors then compared their codebooks and interview notes, resolved disagreements, and merged them into a shared preliminary codebook. Using this merged codebook, they independently coded two additional randomly selected transcripts and further refined the codebook by discussing and clarifying definitions and adding new codes. This iterative process continued, and after the twelfth transcript, no substantial new codes emerged, indicating code saturation [69]. The two authors then used the finalized codebook to re-code all transcripts. Inter-rater reliability was assessed using Cohen's unweighted κ, yielding $\kappa = 0.84$, indicating strong agreement [101]. Any remaining disagreements were discussed and resolved by consensus. The finalized codes were subsequently organized into themes according to our RQs. Due to the primarily qualitative nature of this study, our goal is to characterize patterns in participants' experiences rather than produce precise population estimates. Thus, we use verbal qualifiers (a few (1–3), some (4–6), many (7–12), almost all/all (13–14) [115]) instead of exact counts to avoid a misleading impression of statistical precision.

Gender	Residence	Age	Education	Exp. (yrs)	App Availability	Downloads	Ratings	Team size	Responsibilities (multi-choice)
Woman (6)	UK (5)	18-25 (1)	High school (1)	1-5 (6)	Africa (9)	< 10K (4)	< 1K (2)	1-5 ppl (3)	Software Engineering/Architecture (7)
Man (8)	Germany (5)	26-35 (4)	Associate (1)	6-10 (2)	Asia (8)	10K-1M (2)	1K-10K (3)	11-25 ppl (2)	Security/Privacy (7)
	US (2)	36-45 (5)	Bachelor's (5)	11-15 (5)	Australia/Oceania (8)	1M-50M (2)	10K-30K (2)	26-100 ppl (5)	UX/UI Design & Research (7)
	Argentina (1)	46-55 (3)	Master's (6)	≥ 16 (1)	Europe (10)	≥ 50M (3)	≥ 30K (3)	≥ 101 ppl (4)	Technical Project Management (7)
	Lithuania (1)	≥ 56 (1)	Doctoral (1)		North America (11)		Unavailable (1)		Executive-level Management (4)
					South America (8)				Product Management (4)
									Quality Assurance (4)
									Data Science (3)
									Policy/Legal Compliance (3)
									Marketing (2)

Table 1: Aggregated demographic and professional characteristics of the 14 FemHealth app product team members in this study. Abbreviations were applied to selected terms for clarity and conciseness. The "Education" column reports the number of participants whose highest completed education corresponds to each level. The "Exp. (yrs)" column reports the number of participants with a given range of experience in mobile app design or development. The "App Availability" column indicates the number of unique apps available in each region. The "Downloads" column reports the number of unique apps falling within each download range on Google Play as of April 15, 2026, and the "Ratings" column reports the number of unique apps within each rating range on the App Store as of April 15, 2026. Participants could report multiple responsibilities.

3.5 PSS Requirements Analysis

We used the PRIPARE (Preparing Industry to Privacy by Design by Supporting its Application in Research) framework [129] to perform PSS requirements analysis based on our findings. PRIPARE was initially proposed for privacy engineering, including the analysis of privacy requirements. This framework integrates PbD best practices and standards, and balances high-level expectations (e.g., from regulations) with industry realities. We chose this framework because it is closely relevant to our topic (i.e., PSS perspectives in product teams), and it stands out from other frameworks due to its methodological approach and emphasis on multiple stakeholders [17, 27, 129, 156]. In §5.2, we use two complementary perspectives in the PRIPARE framework (i.e., goal-oriented and risk-based perspectives) to frame our findings into three PSS requirements. In §5.3, we use the PRIPARE framework to bridge requirements to practices and propose recommendations to address the PSS requirements identified in this study.

3.6 Limitations

Our interview findings are based on self-reported data and are therefore subject to recall error and social desirability bias [124]. To mitigate these risks, interviewers avoided leading questions and repeatedly reassured participants, both before and during the interviews, that there were no right or wrong answers. Second, the cross-sectional design of our study, drawing on participants from diverse backgrounds at a single point in time, captures only a snapshot of current practices and perceptions and cannot assess how product teams adapt to legal, regulatory, political, or market changes over time [172]. Although our sample size is small for drawing statistical conclusions, it aligns with qualitative research guidelines that prioritize depth and analytic richness over statistical generalizability [190], and is consistent with prior qualitative security and privacy studies, especially with hard-to-recruit populations such as product teams [e.g., 9, 35, 65, 94, 178]. We also reached data saturation, as described above, by ensuring that the themes identified during our analysis of interview transcripts were sufficient to address our RQs [33], confirming that we derived sufficient meaning from our data to address our RQs and that a larger sample size would have been unlikely to reveal fundamentally new or different themes. Additionally, we did not include participants who spoke languages other than English (e.g., Chinese or Arabic), even though some of these regions have a growing demand for FemTech [146]. Almost all participants (13/14) were based in Europe or North America. This distribution likely reflects both the geographic concentration of FemHealth app teams initially contacted, many of which are headquartered in these regions, and the effects of snowball sampling, as participants often referred peers within their own regional networks. As a result, our sample may not fully reflect the diversity of legal frameworks, regulatory environments, cultural norms, and development constraints in other regions. Future work could address this limitation by expanding linguistic and geographic coverage, for example, through translated interviews or partnerships with regional research networks.

3.7 Author Positionality

All members of the research team have experience in PSS in both academic and industry contexts. Three authors have prior industry experience as product team members, with responsibilities spanning app design and development, general software engineering, and user experience research. All team members have experience working with data from human participants, and three have previously conducted academic research focused on users of FemHealth apps. Three researchers identify as women; notably, two authors have personal experience using FemHealth apps, and one of them was the team member that conducted all participant interviews. We do not aim to make definitive claims about whether FemHealth apps, as a category or individually, are secure, safe to use, or privacy-preserving. Rather, our analysis reflects product team members' perceptions and reported practices, which may differ from the apps' actual technical implementations.

4 Results

4.1 PSS Perspectives and Practices of FemHealth App Product Team Members (RQ1)

4.1.1 ***Data Collection.*** Many participants reported that data collection decisions were not driven by systematic PSS requirements analysis, but rather by functional requirements needed to support core app features. Only after data had already been collected and processed did they begin to consider PSS risks and implement corresponding PSS strategies. The most common reason for data collection, mentioned by almost all participants, was to provide users with the core functionalities of a typical FemHealth app: "*My app needs to collect users' menstrual data to fulfill its main purposes, which are to record past cycles and to predict future ones*" (P11). For many participants, tracking users' health, menstruation, or pregnancy—and, in some cases, predicting menstrual dates or due dates—was viewed as an indispensable feature of FemHealth apps. Interestingly, some participants further suggested that such features and the associated data collection were so ubiquitous that users would already be aware of them, including their PSS implications, without needing to consult privacy statements such as privacy policies: "*Users can read our privacy policy. But no one reads it, which is fine, for everyone knows we need to collect enough data to predict their periods*" (P8).

Moreover, many participants reported that their apps collected users' data to improve the accuracy of predictions generated by their systems: "*We use data to refine our algorithms, thereby improving their accuracy in predictions*" (P7). They viewed accurate predictions about users' bodies—such as menstrual dates, fertility windows, and due dates during pregnancy—as essential features of FemHealth apps: "*All predictions are vital to my users for them to navigate their lives already filled with challenges*" (P14). Some participants further argued that prediction accuracy was so important that it represented users' highest priority, and therefore also the primary focus of their work: "*it is the accuracy, not the privacy or security, that users truly value when selecting FemHealth apps to use*" (P2).

Many participants also reported collecting users' data to provide backup functionality, which they believed was a key user expectation and a contributor to product competitiveness: "*Backups are important to our success. We sometimes receive emails from users asking to recover their accounts. Users may have forgotten their passwords, changed their email addresses, or lost their phones*" (P12). As P12 described, participants believed users expected their data to be linked to cloud-based FemHealth accounts rather than being tied solely to physical devices via local storage, enabling access across multiple devices or after device replacement, with or without access to the original device. Furthermore, they assumed that users also expected to regain access to their data after reinstalling the app on the same device, which further necessitated backup mechanisms: "*Users open an account with us and automatically believe their data will exist as long as they don't delete their account, even after they uninstall our app*" (P2).

Many participants reported collecting data to better understand their user base, including users' preferences and behaviors: "*We prepared two privacy policies with different wordings and presented them to two sets of users, analyzing the time users used to read these two versions*" (P4). They further described using such data to construct user personas based on shared attributes across user segments in order to deliver personalized features: "*Getting to know each individual user and making their personas, we can offer personalized services, which is our greatest selling point*" (P6). Moreover, many participants reported that the apps they worked on collected users' data to share with third parties for data management or storage, analytics, or other service provision: "*We use AWS* [5] *[... and] Auth0* [6]" (P13) and "*We use Cloudflare* [7] *[...] We rely on AppsFlyer* [8] *for marketing and efficiency analysis*" (P1). Some participants reported sharing anonymized user data for research purposes: "*We collaborated with a university to study the effect of COVID-19 vaccines on periods [...] using anonymous data*" (P9). While many participants stated that their apps had never sold and would never sell user data, a few—primarily from smaller product teams—reported sharing user data with third parties for advertising purposes: "*Users cannot get harmed by me sharing their data just for advertisements. My security officer and I needed to get paid. I tried to make a paid version, but then people just didn't download my app*" (P11).

> **Key Takeaway:** FemHealth app product teams largely viewed data collection as feature- and business-driven rather than PSS-requirement-driven decisions, prioritizing data tracking, prediction accuracy, backups, user research, and personalization over PSS implications. This may normalize more extensive data collection and service-side data retention as necessary to maintain service quality, with some participants also citing third-party advertising requirements, further amplifying potential PSS risks.

4.1.2 ***Employed PSS strategies.*** All participants reported that they recognized the sensitivity of the users' data they handled, that they valued users' PSS highly, and that they considered it a professional and moral obligation to protect users' PSS: "*Since it's my job to contribute to this app, I need to make sure it's safe for my users for me to sleep at night*" (P6). They generally perceived no meaningful distinction between FemHealth apps and other types of apps in terms of data sensitivity, and therefore felt equally responsible for protecting PSS in both contexts.

Many participants reported employing PSS strategies they described as "*best practices for common apps*" (P1). These practices included maintaining transparent and comprehensive privacy policies, complying with relevant regulations, minimizing data collection to what was necessary for delivering core functionalities, and providing fine-grained privacy settings: "*We said everything in our privacy policy. [...] We follow regulations based on users' jurisdiction. [...] We respect our users' rights to their data. They can delete their data, and we have data minimization*" (P1); "*We make our privacy settings more fine-grained after the overturn of the Roe v. Wade*" (P13). However, participants differed in their mental models of what constitutes "best practices," how transparent and comprehensive their privacy policies are, what data is strictly necessary, and where the boundaries of data minimization should be drawn. Moreover, these

[5] https://aws.amazon.com
[6] https://auth0.com/
[7] https://www.cloudflare.com/
[8] https://www.appsflyer.com/

mental models may not align with users' expectations. We discuss this further in §5.1.

Except for some participants who were unsure whether data was encrypted in transit, all others reported using traffic encryption. The only form of data encryption *at rest* mentioned by participants was E2EE. Participants described using E2EE to limit their own access to users' data, with users' devices acting as both endpoints for generating and decrypting plaintext, such that only encrypted data is transmitted and stored by product teams.

However, many participants did not use E2EE because they believed that they could offer better and more personalized services to their users if they retained the ability to fully access users' data. Some participants said that their FemHealth apps collected users' data to share it with third parties for advertising purposes; thus, they did not employ mitigation strategies like E2EE, as it would limit their capability to read users' data.

Further, some participants reported performing data classification. By storing different types of data separately according to their usage, teams enforced differentiated access rights so that each team member could only access data necessary for their role: "*We have so many types of users' data: cycles, bleeding patterns, pill usages, sleep data, moods, sex drives, ages, and bowel movements [...] Based on how it will be used, we store our data in different places. For example, one database stores data for user research, one for login credentials*" (P4). Many participants also relied on third-party services, including cloud providers and user identity management providers. When such services were mentioned, some participants acknowledged that they could introduce PSS concerns and stated that they held these third parties accountable for maintaining appropriate PSS standards: "*We choose our service providers carefully and inform them of our strict privacy and security standards*" (P8).

One participant in a small product team (P3) reported that the app they worked on, branded solely for tracking menstrual cycles and not intended to generate revenue, collected data *only* to provide basic features such as tracking and predicting menstrual cycles. Most of the collected data was processed and stored solely on users' devices to enable local predictions, except for a limited amount of anonymized aggregated analytics data, which was transmitted for analysis by P3: "*I do not store users' data on my side, except for a tiny amount of aggregated data. Although I know little about security, I do not have users' data*" (P3). P3 acknowledged that users would lose their data if they lost their phones, as no cloud backup was provided. Except for P3, all other participants either stored users' data solely on servers or used a hybrid approach in which data was stored both on users' devices and on servers via synchronization. Many relied on third-party cloud storage services, while others used in-house servers maintained by the app teams. The primary motivation for using server-side storage was to enable backup functionality.

Regardless of the practices employed by participants, all expressed confidence that their PSS measures were sufficient to protect users. While some acknowledged that improvements were always possible, none reported concerns that their current PSS practices might be ineffective or inadequate: "*There is always room for improvement, but users should not be worried because we are good enough*" (P8). Participants provided various reasons for this confidence, including the absence of user complaints related to PSS issues in their apps: "*We have been very careful about our security and privacy measures, and we have never received any complaints about our non-existing breaches or non-existing safety issues for our users*" (P2). Some participants also attributed their confidence to the professionalism and goodwill of their teams, assuming that no PSS issues would arise as everyone was doing their best to protect users' PSS: "*All of my colleagues are good and genuine. My daughters and I are all using our FemHealth app. Our company has made its best effort to ensure our app is secure and our users are safe*" (P10).

Some participants justified their confidence in PSS protections through compliance with regulatory or privacy and security standards. They believed their apps were safe from PSS risks because they complied with the General Data Protection Regulation (GDPR), even when some users were not located in Europe, arguing that "*many laws seem to follow the steps of GDPR, which is the strictest regulation among all relevant ones*" (P13). A small number of participants referred to other regulations, including the California Consumer Privacy Act (CCPA) and the Personal Information Protection Act (PIPA) in South Korea. Finally, a few participants whose apps were certified under ISO/IEC 27001 or ISO/IEC 27701:2019 believed that such certifications ensured sufficient PSS protections for users: "*We have volunteered to get certified by two ISO certifications, which makes our app the most secure*" (P10).

Key Takeaway: Product teams expressed strong commitments to protecting users' PSS and reported employing a range of protective measures, including privacy settings, access controls, and E2EE. In practice, however, storage and encryption decisions were often shaped by product objectives such as personalization, analytics, and backup functionality, leading many teams to retain server-side access to users' data. Participants were generally confident that their PSS protections were sufficient, frequently basing this confidence on the absence of user complaints, trust in their teams' intentions and expertise, compliance with regulations, or attainment of ISO certifications.

4.2 PSS Challenges Faced by FemHealth App Product Team Members (RQ2)

4.2.1 ***Perceptions of the Uniqueness of FemHealth Apps.*** Our participants expressed three distinct opinions about whether FemHealth apps posed a unique set of PSS risks to their users and whether they should employ additional PSS strategies beyond those commonly used in other, non-FemHealth-related mobile apps.

Firstly, some participants believed that FemHealth apps faced a unique set of PSS threats and, therefore, required distinct PSS practices to adequately protect their users. They attributed these unique threats to the stigma surrounding FemHealth, criminalization risks associated with reproductive health policies, and presence of unique threat actors, including groups and individuals with certain political or religious views, businesses that could misuse FemHealth-related information (e.g., insurance companies), and authorities that might seek evidence of abortions or other forms of conduct: "*My app is a FemHealth app, and its data could be easily used to put a user in jail. We need to have different security measures*" (P7) and "*We will always choose to stand beside our users instead of governments or*

conservative groups, which is the most important thing for product team members of a FemHealth app in today's world" (P14).

Secondly, some participants believed that FemHealth apps were unique in terms of the PSS risks they posed, but did not believe that they required different PSS practices from other apps. They argued that common PSS protection strategies were sufficient to make all apps, including FemHealth apps, adequately secure and privacy-preserving, regardless of the app's genre, focus, or relevant threat actors: "*Risks of FemHealth apps were different from others, but the goal was the same, which was to protect users' data. So there was no need to act any differently than other kinds of apps*" (P2). They also did not believe that users expected FemHealth apps to employ additional or specialized PSS protections, arguing instead that users simply expected FemHealth apps to provide a level of PSS comparable to that of other apps they regularly used: "*Users do not care what we have tailored just for FemHealth apps. Instead, they based their trust on easily identifiable indicators that are also suitable for other apps. For example, if the privacy setting is fine-grained*" (P13). Some participants further stated that they were unsure what additional strategies, beyond commonly accepted practices, could be implemented to address the unique risks associated with FemHealth apps: "*Privacy risks faced by FemHealth apps are definitely unique, [...] but we can only try to follow data protection best practices of data protection made for common apps, I mean, one may say that our best effort is enough*" (P1).

Thirdly, some participants believed that it was illogical to assume that FemHealth data, including menstrual and pregnancy data, could generate sufficiently strong or justifiable suspicions of abortion to influence legal decisions. They argued that many alternative and legitimate explanations could account for user behaviors or patterns in the data. For example, users might stop logging the dates of their menstrual cycles because they forgot or no longer wished to do so, while users might discontinue pregnancy tracking because they no longer found digital logging useful. These participants further argued that users were more likely to leave stronger evidence of abortions in other types of apps than in FemHealth apps, including online messaging apps (e.g., chat histories discussing abortions with friends), navigation apps (e.g., location histories showing visits to particular clinics), web browsers and search engines (e.g., searches about how to obtain or perform abortions), and note-taking or journaling apps (e.g., entries describing abortion-related experiences). Consequently, these participants expressed frustration that they had to devote considerable effort to addressing what they viewed as disproportionate user concerns about the PSS risks of FemHealth apps: "*As a woman and also a FemHealth app user, I knew too well that there could be so many reasons for my periods to be late, and I could just be lazy to continue logging my pregnancy. I sincerely do not believe governments or law enforcement would bother to target FemHealth apps when they could know more about a potential abortion by looking up other things, including a Google map search on gynecological clinics and messages sent. However, apparently, users did not believe this, so we had to persuade our users that our app was safe. We do not know what to do; users are worried, but we are confused*" (P5).

Key Takeaway: Product teams held diverse views on whether FemHealth apps are unique from a PSS perspective compared to non-FemHealth apps. Some believed that FemHealth apps face distinct PSS threats and therefore require additional protections, while others viewed existing PSS practices as sufficient. This lack of consensus, combined with the absence of FemHealth-specific regulatory requirements or standards, contributes to substantial variation in the level of PSS protection provided across FemHealth apps, leaving many users exposed to potential PSS risks and uncertain about the protections offered by the apps they use.

4.2.2 *Challenges in Earning Users' Trust and Maintaining App Availability.*

Many participants observed a decline in user trust in FemHealth apps following changes in legal and regulatory protections related to reproductive rights or access to abortion, as well as increased social media coverage (e.g., reports of legal cases against popular FemHealth apps regarding user privacy). These legal and regulatory changes, together with the polarized political landscape among U.S. politicians, affected FemHealth app usage decisions not only among users in the U.S., but also in Europe: "*Many of our users stopped using our app after the elections in the U.S. at the end of 2024, even though we are based in the EU*" (P4). All our participants were concerned about user trust, as they considered users to be their most important stakeholder: "*Users are the first, final, and most important judges of our app*" (P7). Depending on their views regarding the uniqueness of FemHealth apps' PSS (see §4.2.1), participants differed in whether they considered such user vigilance reasonable. If participants did not believe that FemHealth apps posed unique PSS risks or required additional PSS strategies, they also did not view users' concerns as justified, and vice versa. Furthermore, some argued that users' concerns about FemHealth apps were disproportionately amplified by social media and should be addressed through user education: "*Users need to be educated on how their browsers work regarding advertisements. We have never shared users' data, but they might have left a footprint by searching pregnancy-related content. They are too sensitive and worried because of the news they read*" (P10).

Some participants were concerned that if users no longer trusted their apps, those apps would fail as businesses would be forced to exit app marketplaces and would no longer be able to provide continuous services. Participants expressing this concern came from both small and relatively large product teams: "*Although we have a large user base and some granted funding, it's difficult to keep the company going and become self-sufficient. Our users, however, don't seem to worry about us failing as a company and thus losing all their data*" (P5) and "*Our business model is built on subscriptions and not on users' data, so that users can trust us, a win-win situation. If they stop trusting us, our services will no longer be available, a loss-loss situation*" (P14).

To earn users' trust, many participants reported that their apps sought to communicate the PSS risk mitigation strategies they employed and the due diligence they undertook to protect users. The methods used to communicate PSS strategies are also commonly used in other types of apps, including disclosures of data practices

in privacy policies and privacy nutrition labels (e.g., Data Safety sections in Google Play, or App Privacy sections in the Apple App Store). Additional explanations in app marketplace descriptions were also used, along with evidence provided on app web pages or in in-app articles, responses to users' public reviews and comments on app marketplaces or online forums, emphasis on PSS protections in app advertising on social media, and user research conducted to communicate practices to selected participants.

However, many participants still believed that these efforts were insufficient to convince users and that they had not succeeded in earning users' trust: "*No matter what we do, it takes only one negative report on social media that is compelling and seemingly correct, for us to lose users' trust*" (P1) and "*I do not know how to convince our users that they and their data are safe with us*" (P14). In addition to the perceived ineffectiveness of these methods, many participants criticized the lack of meaningful PSS standards tailored to FemHealth apps that could serve as evidence of their diligence. For some participants, this absence of FemHealth-specific standards also meant insufficient guidance on how to develop secure, privacy-preserving, and safe FemHealth apps. Some participants also did not find existing security standards, such as ISO/IEC 27001 and ISO/IEC 27701:2019, particularly useful for FemHealth apps: "*ISO or some medical device certifications are not designed for our app. When I filled out some of their forms, I had no choice but to improvise*" (P7) and "*Some apps got certified by ISO 27001 and 27701, but they are cumbersome to get and are not designed for our kind of apps*" (P4).

Nevertheless, some participants were not concerned about their apps' potential failure as businesses, even if they could not convince their users to trust their PSS protections. They believed that although users might not trust their apps' PSS protections, they would still choose to use the apps due to the convenience and utility of the apps' features and functionalities. In other words, these participants argued that users would often disregard PSS concerns in order to access services they needed or wanted: "*People know cookies are unhealthy, they eat them anyway. Similarly, users and social media platforms frequently discuss their great privacy and safety concerns, but in reality, users never act on these concerns*" (P6).

Key Takeaway: Changes in legal and regulatory protections of reproductive rights, together with social media coverage of these changes, have made user trust fragile, with some product teams reporting user loss even in safer jurisdictions. Our product team participants tried various trust-building strategies, but many felt these were undermined by persistent negative narratives in public discourse and the lack of FemHealth-specific PSS standards. Others downplayed the risks, assuming that users would ignore PSS concerns and continue using their apps to receive services they wanted or needed.

4.2.3 ***Challenges in Complying with Data Privacy Regulations and Reproductive Rights Policies.*** Many participants did not know how to comply with both data privacy regulations and reproductive rights policies, although all of them felt pressured to hand over users' data in case of subpoenas. They were unsure whether they should provide users' data to law enforcement if asked, or whether they should even be technically prepared to do so before such requests were made. Many participants perceived a tension between reproductive rights policies, which could require FemHealth apps to provide users' data, and data privacy regulations, which require protecting users' data, with no clear path for satisfying both requirements: "*Protecting users' privacy and offering evidence for court cases cannot both be of highest priority*" (P10).

Some participants were uncertain whether the legal stance of their FemHealth apps should differ from that of non-FemHealth apps. They questioned whether they should prioritize compliance with reproductive rights policies at any cost, given their perceived specificity to FemHealth contexts, compared to data privacy regulations, which are more general and applicable across app domains: "*We follow GDPR, but as no data protection laws can be specific to our area, we have to adapt*" (P6) and "*Anti-abortion laws conflict with data privacy laws and our commitment to our users, but it feels that it's a law closer to our app. It's confusing*" (P11).

At the same time, participants held differing views on compliance obligations across jurisdictions. Specifically, when users resided in or were citizens of country A while the company headquarters and data storage were located and registered in country B, participants differed in whether they needed to comply with regulations from both countries A and B, and how to resolve potentially conflicting requirements or guidance. Some participants believed that as long as data privacy regulations in country B required them to protect users' data, they did not need to disclose users' data in response to subpoenas from country A.

On the other hand, some participants believed that being registered in country B did not exempt them from legal requirements or subpoenas from country A, as long as they had users residing in or holding citizenship in country A, although their confidence in their legal understanding and ability to handle such cases was limited: "*It's complicated because we also have American users. Luckily, we did not have to cross this bridge because no one has asked us for data so far, although we do not really know what to tell our users*" (P4). Almost all participants emphasized that they did not have a clear answer on how they would respond if asked to provide users' data to authorities, as such decisions would require case-by-case consultation with legal counsel, given the lack of accessible FemHealth-app-specific guidance on permissible actions and decision-making processes. This uncertainty also made it difficult for teams to be transparent with users about their legal stance on data sharing with authorities.

Key Takeaway: Product teams faced compliance challenges on two fronts. First, they expected pressure to disclose user data under certain reproductive health-related policies, which could conflict with data privacy obligations, leaving them uncertain about how to respond to subpoenas. Second, they held conflicting assumptions about cross-border jurisdiction, reinforcing ad hoc, case-by-case decision-making rather than formalized strategies and making their PSS stances unclear to users.

4.2.4 ***Challenges with Technical Capabilities.*** Some participants, from both large and small product teams, reported technical challenges in implementing PSS guarantees (see §4.1.2), particularly

for backup features: "*Recently, we have decided not to store data on users' devices and only back it up in the Cloud, because having both requires us to do data synchronization, which is technically difficult*" (P14). Several participants also noted that backups could be implemented more easily by allowing users to download or receive an email containing their data (i.e., data export features outside FemHealth apps): "*Some users don't care about recovering or maintaining their account, but just want to get a PDF version of all of their period-related data to download and perhaps to print out as a physical backup*" (P12).

In addition, some participants described technical difficulties in implementing and maintaining E2EE. They felt that E2EE limited their ability to access users' data flexibly, requiring additional mechanisms to meet both product and user needs. For example, one participant explained that encryption keys were currently known only to users, meaning that if users lost their keys, they would permanently lose access to their accounts and all associated data: "*They can store their encryption keys at various places, like Chrome password managers. Nevertheless, because we do not have control over their encryption keys, we cannot prevent them from losing their keys or access to their accounts. Indeed, many users complained of losing their accounts and data*" (P9).

One participant acknowledged difficulties in implementing complex PSS guarantees that would address risks related to multiple threat actors simultaneously: "*It's difficult because it's like we are fighting against everyone: nosy governments, bad police, religious groups, individuals with different opinions than our users, users' controlling family and fake friends*" (P2). Some participants discussed their apprehension about how to technically address risks posed by actors with physical access to users and their devices, including violent and manipulative intimate partners, police who might use physical force and mental intimidation to obtain evidence, parents who control and access their children's devices, and friends who share users' mobile phones: "*I can force my wife to open or re-download her app and show all of her data. I know such men in my life, and I don't know what to do as a product team member*" (P4). Some participants also noted that such actors complicated user authentication during account recovery: "*Users expect us to be able to recover their account. However, a password resetting email can potentially be sent by a user's over-controlling parents or ill-intentioned friends*" (P5).

Key Takeaway: Product teams identified technical difficulties in implementing strong PSS protections: features expected by users (especially backups) introduced challenges with synchronization, cloud storage, and account recovery. Although E2EE was seen as desirable, it was perceived as operationally fragile due to risks of permanent data loss in case of lost keys, making it difficult to balance PSS guarantees with usability and support. Teams also reported a lack of FemHealth-specific PSS guidance, particularly for defending against high-risk local adversaries with physical access to users' devices.

5 Discussion

5.1 Implications of Key Findings

Previous studies have emphasized the high PSS risks posed by FemHealth apps due to the sensitivity of the data they collect from users [11, 56, 120]. Users are often aware of such sensitivity and express strong PSS concerns [38, 119, 170]. We found that all our participants also recognized that they handle sensitive data (see §4.1.2). However, we identified a gap in PSS requirements analysis: FemHealth app product teams often operationalize "sensitivity" in a generalized way, overlooking the distinct threats posed by FemHealth data and assuming all user data is equally sensitive. In contrast, many computer security researchers argue that FemHealth apps pose distinctive PSS risks [38, 111]; for instance, inferences from FemHealth data could reveal a potential abortion, which may be punishable in some jurisdictions [66, 107, 165], and may motivate different threat actors, including authorities and intimate partners, to seek access to such data [117, 165]. However, some legal scholars, as well as some of our participants, questioned whether FemHealth data alone provide sufficient strong evidence to justify investigative or legal action, given the many benign explanations for missing or irregular period records [7, 8, 54, 55, 64, 97, 104]. From a PSS perspective, the key issue is therefore not whether FemHealth data is uniquely evidentiary in isolation, but whether it becomes personally identifiable and interpretable when combined with other data (e.g., location or chat history), shifting the question of "uniqueness" from a categorical claim to an engineering or technical question about linkage, retention, and access paths. As a result, participants' views on whether FemHealth apps require unique PSS requirements and specialized protections compared to common apps differed significantly (see §4.2.1), and this lack of consensus is consequential because it shapes which adversaries are considered relevant, which attack surfaces are prioritized, and what constitutes effective mitigation practices.

A large-scale user review analysis found that 2022 marked a transition from predominantly positive to predominantly negative sentiments about FemHealth apps among users, with privacy, data processing, and the overturning of *Roe v. Wade* frequently discussed as key concerns [125]. Prior work has documented concrete PSS risks extending beyond abortion inference alone, including inadequate or manipulative consent practices [10, 111], shifting of PSS responsibility onto users [111], poor transparency and limited comprehension of privacy disclosures [60, 158], restricted user control and lack of fine-grained privacy settings [79, 118], and inconsistencies between FemHealth apps' disclosed and actual practices [111]. Despite these risks and shifts in reproductive rights policies and user sentiments regarding PSS, many product teams reported making little change beyond standard compliance and baseline technical controls (see §4.1.2 and §4.2.4), thereby widening the gap between user expectations and implemented PSS protections in FemHealth apps. Moreover, some of our participants assumed that users of the FemHealth apps they worked on fully understood the PSS implications of using these apps (see §4.1.1). However, prior user research [e.g., 79, 90, 111, 170] has shown that while users tend to have relatively accurate awareness of data they directly input (such as menstrual dates or symptoms), their mental models of less visible

data collection (such as sensor-derived or location data) and of potential inferences drawn from such data (including about possible abortions or medical conditions) are considerably less accurate.

Although our participants described the PSS practices of their FemHealth apps as sufficient and framed further improvements as non-essential (see §4.1.2), the reasons they provided are questionable. First, the absence of user complaints does not necessarily indicate that PSS protections are effective. Users do not have access to the same level of information as product teams (e.g., backend logs used to detect abnormal data flows) and typically lack the professional knowledge about PSS protection that product teams are expected to have, making it difficult for them to assess the presence and effectiveness of implemented safeguards. Further, many PSS violations can remain unnoticed even by experts [18, 89, 112]. Second, good intentions and best efforts by product teams do not necessarily lead to adequate PSS protections, and their perceptions of the effectiveness and sufficiency of the protections they implemented can differ from both technical reality and users' expectations of adequate safeguards. For example, while many participants believed they were following best PSS practices—such as providing transparent privacy policies, offering fine-grained privacy settings, and applying data minimization principles—prior studies have shown that privacy policies are often insufficiently transparent and comprehensive [60, 158], unnecessary data (e.g., location data) is commonly collected [10], and privacy settings are not sufficiently fine-grained [79, 118]. Third, although regulations and standards provide some guidance, without continuous formal assessment or auditing, product teams cannot be certain that their apps remain compliant with those requirements or consistently adhere to them over time. This seemingly unjustified view is concerning because FemHealth app product teams operate in a threat landscape where (i) political and legal actors could become adversaries with little warning (e.g., a subpoena issued from a jurisdiction different from where the product is based), (ii) local access adversaries (e.g., intimate partners and law enforcement) are routinely in scope, and (iii) core product features can introduce significant PSS risks (e.g., failed backups affecting data availability, or weak authentication and account recovery mechanisms compromising privacy). Furthermore, our findings suggest that many teams treat PSS as an "afterthought," addressed only after users' data has already been collected and processed (see §4.1.1), relying primarily on general technical safeguards and compliance practices rather than explicit, adversary-scoped PSS requirements analysis (see §4.2).

5.2 PSS Requirements Analysis for FemHealth Apps via PRIPARE Framework

To translate our findings into actionable PSS engineering artifacts, we drew on the PRIPARE framework [129] to articulate PSS goals and risks that support PSS requirements analysis for FemHealth apps. Although PRIPARE was originally developed for privacy engineering, its close conceptual ties to security and safety make it well suited to our context. We applied PRIPARE's two complementary lenses—goal-oriented and risk-based requirements analysis—to surface what was often implicit in our participants' accounts: expectations about which stakeholder needs must be satisfied, which adversaries and risks must be considered, and what product teams require to address them. We outline this PSS requirements analysis in this section and provide recommendations in §5.3.

From a *goal-oriented* perspective, our participants consistently identified users as the primary stakeholder, yet many struggled to earn and sustain user trust amid political or regulatory changes and social media amplification of PSS concerns (see §4.2.2). For example, many FemHealth apps failed to employ sufficient PSS protections and to clearly articulate their legal positions regarding data sharing with authorities following the overturning of *Roe v. Wade* [51, 99, 111, 168]. This points to **the first PSS requirement: FemHealth apps should be demonstrably trustworthy. Specifically, FemHealth app teams should maintain clear documentation and auditable logs for independent review, and provide users with clear, accessible information that enables them to understand and trust what data is collected, how it is protected, and which organizations or individuals can or cannot access it.**

From a *risk-based* perspective, previous studies [2, 52, 143, 148, 168, 187, 192] and our findings (see §4.2.4 and §4.2.1) highlight adversaries that may not be relevant for other genres of apps, but are salient in FemHealth app contexts, including local actors with physical access or coercive power (e.g., family members and friends), groups and individuals with particular views, businesses (e.g., insurance companies), and, in some jurisdictions, authorities seeking evidence related to app users' sexual and reproductive health (e.g., governments and law enforcement). We further found that our participants worked with various kinds of users' data, including menstruation, pregnancy, mood, and sleep patterns (see §4.1.2). This motivates **the second PSS requirement: FemHealth app product teams should systematically manage PSS risks across all types of users' data, while accounting for adversaries with diverse capabilities, motivations, and levels of access**.

Finally, PRIPARE emphasizes legal compliance as an important consideration for risk-based requirements analysis. Yet, our FemHealth app product team participants expressed substantial uncertainty regarding legal requirements, particularly in cross-country contexts, and reported difficulties in complying with them, especially when data protection obligations may conflict with policy requirements related to reproductive rights and cross-border data requests (see §4.1.2 and §4.2.3). This motivates **the third requirement: FemHealth app product teams should have clear operational guidance to support jurisdiction-aware compliance efforts (e.g., subpoena-handling policies and technical mechanisms such as E2EE configurations that enable controlled access to users' data when legally required).**

PRIPARE helps reframe our findings as a FemHealth-app-specific PSS requirements problem. In summary, the challenge does not lie in FemHealth app product teams' motivation to protect users' PSS, but rather in how they can specify and adhere to adversary-scoped PSS requirements that align product functionality (especially backups, recovery, and personalization) with diverse threat actors and legally grounded constraints.

5.3 Recommendations for Addressing PSS Requirements

Building on the PSS requirements analysis (see §5.2), in this section, we translate our findings into two complementary sets of recommendations: (i) technical recommendations for FemHealth app product teams to operationalize PSS requirements in design and development, and (ii) policy and governance recommendations to reduce uncertainty around legal obligations for product teams and support their interpretation of and compliance with regulations.

5.3.1 Technical Recommendations for Product Teams. Firstly, to support FemHealth app product teams' efforts in building or maintaining user trust and managing PSS risks, we recommend a hierarchical data classification scheme that ranks data types by their potential for harm under realistic threat actors and maps each data type to concrete PSS strategies. Although our participants already used forms of data classification (see §4.1.2), data was primarily classified based on usage context (e.g., account recovery, analytics and product improvement, or vulnerability discovery) and primarily for internal access control within product teams. While our proposed scheme also accounts for the diverse types of data processed by FemHealth apps (see §5.2), we further recommend classifying and prioritizing data based on the severity of PSS risks posed under different threat models. We also recommend explicitly mapping each data type to corresponding PSS strategies. Such a scheme can serve as a starting point to facilitate users' understanding of and trust in apps' data practices, thereby addressing the first PSS requirement. Although no PSS protections should be designed under the assumption that adversaries are unaware of system mechanisms (e.g., adversaries should be assumed to know the encryption scheme used for data transmission), product teams may still choose not to disclose certain implementation details for pragmatic reasons (e.g., maintenance costs associated with keeping public documentation up to date). Nevertheless, maintaining a structured hierarchical data classification scheme ensures that relevant information is readily available for public disclosure when needed. For example, teams may classify menstruation and pregnancy data as high risk, and device diagnostics as lower risk. Crucially, the classification should also specify which adversaries are relevant for each data type (e.g., governments for pregnancy-related inferences and intimate partners for sexual activity–related risks) and which PSS protections are applied to each category (e.g., E2EE for pregnancy status data and strict internal access controls for sexual activity data). To mitigate potential errors and biases in the implementation of such classification schemes, we recommend following established privacy and security risk assessment guidelines [127, 153, 159] and conducting regular independent audits by security experts [42, 100, 121].

Secondly, our findings show that backup capabilities strongly shape teams' decisions about storage and encryption, yet teams face significant engineering constraints when implementing and maintaining E2EE and recovery workflows (§4.2.4). Echoing Malki et al. [111] and drawing on empirical evidence from our findings, we argue that backup and recovery should be treated as PSS-critical workflows requiring explicit design attention and documented failure handling. Product teams should clearly specify the recovery guarantees they provide, the failure modes users may encounter (e.g., loss of authentication tokens), and the trade-offs they accept between recoverability and confidentiality. Where E2EE is employed, product teams should consider PSS-preserving recovery mechanisms (e.g., multi-device key management or carefully scoped escrow models) and clearly communicate residual risks to users [46, 77]. Beyond backup and recovery, product teams should shift from treating PSS as an afterthought (see §4.1.1) to adopting proactive, preventive approaches, embedding PSS protections following PbD principles [40].

Thirdly, our participants expressed difficulties in defending users against actors with physical access to devices (e.g., intimate partners, parents, or police) (§4.2.4). Beyond backend protections, product teams should incorporate interface-level PSS mechanisms aligned with realistic coercion scenarios, such as discreet modes, rapid data hiding or deletion, multi-level authentication mechanisms for particularly sensitive or high-risk data, granular control over log visibility, threat-aware authentication defaults, and carefully designed export features. Importantly, user-exported backups (e.g., downloadable PDFs or emailed records) may reduce server-side retention but can increase exposure to local threat actors (e.g., access to email accounts or device storage) and weaken the effectiveness of deletion, as exported copies persist outside the app. Teams should therefore explicitly account for post-export risks as part of the PSS design surface, treat data export as a high-risk workflow, and provide in-context warnings and alternatives where possible.

5.3.2 Policy and Governance Recommendations. Prior work has shown that FemHealth app users are concerned about privacy risks and potentially severe legal consequences [102, 116, 152], consistent with prior work [51, 99, 111, 168]. However, our participants from FemHealth app product teams recognized a persistent gap between data protection obligations and perceived pressures arising from reproductive rights policies, as well as a high level of uncertainty among FemHealth app product teams regarding subpoenas and cross-jurisdictional applicability (see §4.2.3). Rather than assuming that such ambiguity can be resolved through technical "best practices" alone, **our participants wanted accessible FemHealth-app-specific guidance** that specifies (i) what constitutes lawful disclosure, (ii) when and how cross-border requests apply, and (iii) which procedural safeguards and transparency obligations should govern government access requests. App marketplaces, policymakers, and regulators can collectively contribute to providing such guidance to product teams. Such guidance would directly support PRIPARE's compliance-focused requirements by enabling teams to move from *ad hoc* decision making to jurisdiction-aware, prespecified disclosure about data sharing with authorities. Even if some or all decisions about sharing data with authorities must be made *ad hoc*, it is still desirable to provide teams with guidance about it, to better inform product teams and provide a reference point for them to earn users' trust.

We also suggest revisiting whether, and how, FemHealth data should receive heightened legal protection. Currently, only a small subset of FemHealth apps fall under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the U.S. due to the narrow scope of what qualifies as "covered entity" and "protected health information" [61]. Given the sensitivity and inferential power of FemHealth data, policymakers should not only

improve existing data protection laws to better serve the complex needs of FemHealth apps [120, 126, 139, 149, 189], but also consider stronger, context-appropriate protections, including whether certain FemHealth data practices ought to be governed under medical data or medical device regulatory frameworks. We do not argue that FemHealth apps must collect less data; rather, we acknowledge that many data collection reasons outlined by our participants are functionally justified (§4.1.1), but require enforceable guardrails around data access, retention, sharing, and disclosure. Across other parts of the world, regulators should similarly revisit whether existing legal frameworks adequately reflect the sensitivity and predictive power of FemHealth app data. For example, while the EU's GDPR offers a good baseline for PSS protections [19, 147], which some of our participants acknowledged too (see §4.1.2), its complexity [85] creates significant ambiguity about how FemHealth data should be protected, particularly when it may fall outside the traditional "data concerning health" definition. Moreover, although GDPR encourages data sharing with law enforcement for purposes such as national security and criminal investigations, this has led to widespread data sharing practices among businesses [199]. Therefore, regulators and policymakers should seek a balance between these provisions in GDPR and FemHealth app users' strong concerns about data sharing with authorities.

Finally, our results highlight the lack of PSS standards tailored to FemHealth apps (§4.2.2). **Standard-setting bodies could address this gap by defining baseline expectations for FemHealth app data minimization, encryption boundaries, default retention periods, disclosures regarding third-party sharing, and procedures for responding to legal demands.** Such standards should recognize the workflow-level nature of FemHealth app risks by treating backups, account recovery, and data export as protected operations with explicit PSS requirements, rather than leaving them to discretionary implementation. Doing so would provide app product teams with more credible ways to demonstrate due diligence beyond generic privacy policies or broad ISO certifications, while also reducing governance blind spots that emerge when stated PSS commitments are undermined by operational or business incentives.

6 Conclusion

FemHealth apps operate at the intersection of highly intimate data, volatile political conditions, and uneven regulatory protections. Through interviews with 14 FemHealth app product team members representing 11 unique apps, we show that teams often approach PSS through generalized notions of sensitive data and compliance-driven best practices, while key product decisions (e.g., backups, account recovery, and personalization) frequently determine an app's overall PSS posture. We identify four challenges shaping FemHealth PSS practices: contested views on the uniqueness of FemHealth apps, difficulties in earning and sustaining user trust, uncertainty arising from conflicting legal regimes and cross-border enforcement, and technical constraints related to backups, E2EE, and coercive local access. We then apply the PRIPARE framework to translate our findings into PSS requirements that are tailored to specific adversaries, aligned with operational workflows, and sensitive to jurisdictional contexts. We recommend that teams adopt threat-actor-aware data classification, treat backup and recovery as core PSS design challenges, and explicitly design for coercive local access. At the governance level, we highlight the need for clearer guidance on disclosure and subpoena handling, FemHealth-specific PSS standards, and regulatory approaches that better address the inferential and contextual risks of reproductive data. Overall, our findings support more actionable, accountable, and context-aware PSS practices in FemHealth app design and development.

Acknowledgments

We thank the PETS reviewers for their insightful feedback, which significantly improved this manuscript. We are also grateful to all of our participants for generously sharing their time and experiences. This research was supported by an unrestricted gift from Google and by the U.S. National Science Foundation under Award CNS-2055772. Chenkai Ma is a Ph.D. student supported by a Faculty of Natural, Mathematical & Engineering Sciences studentship at King's College London.

References

[1] Yasemin Acar, Sascha Fahl, and Michelle L Mazurek. 2016. You are not your developer, either: A research agenda for usable security and privacy research beyond end users. *IEEE Cybersecurity Development* (2016), 3–8.

[2] Lora Adair, Nicole Lozano, and Nelli Ferenczi. 2024. Abortion attitudes across cultural contexts. *International Perspectives in Psychology* (2024).

[3] Amy Adamczyk, Chunrye Kim, and Leevia Dillon. 2020. Examining public opinion about abortion: A mixed-methods systematic review of research over the last 15 years. *Sociological Inquiry* 90, 4 (2020), 920–954.

[4] Gillian I Adynski, Lilian Bravo, Melissa Harris, Harry R Adynski, Sandra Zaragoza, Ebahi Ikharo, Latesha K Harris, and Charity Lackey. 2022. Global implications of Dobbs vs. Jackson Women's Health Organization for nurses as a historically gendered profession. *International Journal of Nursing Studies* 135 (2022), 104342.

[5] Daniel Ajiga, Patrick Azuka Okeleke, Samuel Olaoluwa Folorunsho, and Chinedu Ezeigweneme. 2024. Designing cybersecurity measures for enterprise software applications to protect data integrity. *Computer Science & IT Research Journal* 5, 8 (2024), 1920–1941.

[6] Ala'a Saeb Al-Sherideh, Roesnita Ismail, Mohammad Rasmi Al-Mousa, Khaled Al-Qawasmi, Ala'a Al-Shaikh, Hebatullah Awwad, Khaled Maabreh, and Mohammad Alauthman. 2024. Development of a secure model for mobile government applications in Jordan. *Journal of Statistics Applications & Probability* 13, 1 (2024), 145–155.

[7] Kendra Albert, Maggie Delano, and Emma Weil. 2022. Fear, uncertainty, and period trackers. https://medium.com/@Kendra_Serra/fear-uncertainty-and-period-trackers-340ab8fdff74. Accessed: 2025-08-01.

[8] Kendra Albert, Maggie Delano, and Emma Weil. 2022. Okay, fine, let's talk about period tracking: The detailed explainer. https://medium.com/@maggied/okay-fine-lets-talk-about-period-tracking-the-detailed-explainer-2f45112eebb4. Accessed: 2025-08-01.

[9] Martin R Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. 2021. Collective information security in {large-scale} urban protests: The case of Hong Kong. In *30th USENIX Security Symposium*. 3363–3380.

[10] 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.

[11] Teresa Almeida, Laura Shipp, Maryam Mehrnezhad, and Ehsan Toreini. 2022. Bodies like yours: Enquiring data privacy in FemTech. In *Adjunct Proc. of the Nordic Human-Computer Interaction Conference*. 1–5.

[12] Noura Alomar and Serge Egelman. 2022. Developers say the darnedest things: Privacy compliance processes followed by developers of child-directed apps. *Privacy Enhancing Technologies Symposium* 2022, 4 (2022), 24.

[13] Ashwaq Alsoubai, Reza Ghaiumy Anaraky, Yao Li, Xinru Page, Bart Knijnenburg, and Pamela J Wisniewski. 2022. Permission vs. app limiters: Profiling smartphone users to understand differing strategies for mobile privacy management. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–18.

[14] Bashair Althani. 2025. Migration challenges of legacy software to the cloud: A socio-technical perspective. *Cogent Business & Management* 12, 1 (2025), 2503421.

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

[16] 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.

[17] Vinicius Camargo Andrade, Rhodrigo Deda Gomes, Sheila Reinehr, Cinthia Obladen De Almendra Freitas, and Andreia Malucelli. 2022. Privacy by design and software engineering: A systematic literature review. In *Proc. of the XXI Brazilian Symposium on Software Quality*. 1–10.

[18] Andrea Apicella, Francesco Isgrò, and Roberto Prevete. 2025. Don't push the button! Exploring data leakage risks in machine learning and transfer learning. *Artificial Intelligence Review* 58, 11 (2025), 339.

[19] Emma Arfelt, David Basin, and Søren Debois. 2019. Monitoring the GDPR. In *European Symposium on Research in Computer Security*. Springer, 681–699.

[20] Edna Astbury-Ward, Odette Parry, and Ros Carnwell. 2012. Stigma, abortion, and disclosure—findings from a qualitative study. *The Journal of Sexual Medicine* 9, 12 (2012), 3137–3147.

[21] Audie A Atienza, Christina Zarcadoolas, Wendy Vaughon, Penelope Hughes, Vaishali Patel, Wen-Ying Sylvia Chou, and Joy Pritts. 2015. Consumer attitudes and perceptions on mHealth privacy and security: Findings from a mixed-methods study. *Journal of Health Communication* 20, 6 (2015), 673–679.

[22] Amid Ayobi, Paul Marshall, Anna L Cox, and Yunan Chen. 2017. Quantifying the body and caring for the mind: Self-tracking in multiple sclerosis. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 6889–6901.

[23] Rebecca Balebako and Lorrie Cranor. 2014. Improving app privacy: Nudging app developers to protect user privacy. *IEEE Security & Privacy* 12, 4 (2014), 55–58.

[24] Louise Barkhuus. 2012. The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI. In *Proc. of the SIGCHI Conference on Human Factors in Computing Systems*. 367–376.

[25] Solon Barocas and Helen Nissenbaum. 2009. On notice: The trouble with notice and consent. In *Proc. of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*.

[26] Suzanne O Bell, Alexander M Franks, David Arbour, Selena Anjur-Dietrich, Elizabeth A Stuart, Eli Ben-Michael, Avi Feller, and Alison Gemmill. 2025. US abortion bans and fertility. *JAMA* 333, 15 (2025), 1324–1332.

[27] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proc. on Privacy Enhancing Technologies* (2016).

[28] Amel Bourdoucen and Janne Lindqvist. 2024. Privacy of default apps in Apple's mobile ecosystem. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–32.

[29] Richard E Boyatzis. 1998. *Transforming qualitative information: Thematic analysis and code development*. Sage.

[30] Jane Bradley and Elizabeth Dias. 2025. They helped topple Roe v. Wade. Now their sights are set on Britain. https://www.nytimes.com/2025/10/13/world/europe/uk-abortion-farage.html. Accessed: 2025-10-20.

[31] Virginia Braun and Victoria Clarke. 2013. Successful qualitative research: A practical guide for beginners. (2013).

[32] Virginia Braun and Victoria Clarke. 2019. Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health* 11, 4 (2019), 589–597.

[33] Virginia Braun and Victoria Clarke. 2021. To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health* 13, 2 (2021), 201–216.

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

[35] Mikaela Brough, Rikke Bjerg Jensen, and Martin R Albrecht. 2025. On the virtues of information security in the {UK} climate movement. In *34th USENIX Security Symposium*. 5091–5110.

[36] Victoria Browne. 2025. How to defeat miscarriage stigma: From 'breaking the silence' to reproductive justice. *Feminist Theory* 26, 1 (2025), 203–223.

[37] Adrian Bussone, Simone Stumpf, and George Buchanan. 2016. It feels like I'm managing myself: HIV+ people tracking their personal health information. In *Proc. of the 9th Nordic Conference on Human-Computer Interaction*. 1–10.

[38] 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. (2024).

[39] Valentina Casola, Alessandra De Benedictis, Carlo Mazzocca, and Vittorio Orbinato. 2024. Secure software development and testing: A model-based methodology. *Computers & Security* 137 (2024), 103639.

[40] Ann Cavoukian et al. 2009. Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada* 5, 2009 (2009), 12.

[41] Nai-Yu Cheng, Novia Wong, and Madhu Reddy. 2025. Understanding mental wellbeing and tools for support with Taiwanese emerging adults: An Eastern cultural perspective. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–18.

[42] Jia Hui Chin, Pu Zhang, Yu Xin Cheong, and Jonathan Pan. 2025. Automating security audit using large language model based agent: An exploration experiment. *arXiv preprint arXiv:2505.10732* (2025).

[43] Eun Kyoung Choe, Jaeyeon Jung, Bongshin Lee, and Kristie Fisher. 2013. Nudging people away from privacy-invasive mobile apps through visual framing. In *IFIP Conference on Human-Computer Interaction*. Springer, 74–91.

[44] Partha Das Chowdhury, Joseph Hallett, Nikhil Patnaik, Mohammad Tahaei, and Awais Rashid. 2021. Developers are neither enemies nor users: They are collaborators. In *IEEE Secure Development Conference*. 47–55.

[45] Michael Colesky, Jaap-Henk Hoepman, and Christiaan Hillen. 2016. A critical analysis of privacy design strategies. In *IEEE Security and Privacy Workshops*. IEEE, 33–40.

[46] Graeme Connell, Vivian Fang, Rolfe Schmidt, Emma Dauterman, and Raluca Ada Popa. 2024. Secret key recovery in a {global-scale}{end-to-end} encryption system. In *18th USENIX Symposium on Operating Systems Design and Implementation*. 703–719.

[47] Shanti Das. 2024. 'Extreme' US anti-abortion group ramps up lobbying in Westminster. https://www.theguardian.com/world/2024/apr/06/extreme-us-anti-abortion-group-ramps-up-lobbying-in-westminster

[48] Shanti Das. 2025. 'Unprecedented' rise in abortion prosecutions prompts call for law change from medical leaders. https://www.theguardian.com/society/2025/jan/12/unprecedented-rise-in-abortion-prosecutions-prompts-call-for-law-change-from-medical-leaders. Accessed: 2025-08-26.

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

[50] Sergio Di Meglio. 2025. End-to-end testing in Web environments: Addressing practical challenges. In *IEEE Conference on Software Testing, Verification and Validation*. IEEE, 782–784.

[51] 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. *37th IEEE/ACM International Conference on Automated Software Engineering* (2022), 6.

[52] Christine Piette Durrance, Yang Wang, and Barbara Wolfe. 2024. Do mandatory waiting periods for abortion increase intimate partner violence? *Journal of Health Economics* 98 (2024), 102939.

[53] Anirudh Ekambaranathan, Jun Zhao, and Max Van Kleek. 2020. Understanding value and design choices made by Android family app developers. In *Extended Abstracts of CHI Conference on Human Factors in Computing Systems*. 1–10.

[54] 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 *Proc. of the CHI Conference on Human Factors in Computing Systems*. 6876–6888.

[55] Daniel A Epstein, An Ping, James Fogarty, and Sean A Munson. 2015. A lived informatics model of personal informatics. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 731–742.

[56] Jacob Erickson, Jewel Y Yuzon, and Tamara Bonaci. 2022. What you do not expect when you are expecting: Privacy analysis of FemTech. *IEEE Transactions on Technology and Society* 3, 2 (2022), 121–131.

[57] Ming Fan, Le Yu, Sen Chen, Hao Zhou, Xiapu Luo, Shuyue Li, Yang Liu, Jun Liu, and Ting Liu. 2020. An empirical evaluation of GDPR compliance violations in Android mHealth apps. In *IEEE 31st International Symposium on Software Reliability Engineering*. IEEE, 253–264.

[58] Matthias Fassl, Lea Theresa Gröber, and Katharina Krombholz. 2021. Stop the consent theater. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. 1–7.

[59] Tessa Flemming. 2025. Critics say new UK police guidelines concerning stillbirths and abortions are fuelling a 'culture of hostility'. https://www.abc.net.au/news/2025-05-30/npcc-guidelines-on-stillbirths-abortions-draws-controversy/105332518. Accessed: 2025-10-20.

[60] 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.

[61] Sarah Fox, Noura Howell, Richmond Wong, and Franchesca Spektor. 2019. Vivewell: Speculating near-future menstrual tracking through current data practices. In *Proc. on Designing Interactive Systems Conference*. 541–552.

[62] Othmane Friha, Mohamed Amine Ferrag, Burak Kantarci, Burak Cakmak, Arda Ozgun, and Nassira Ghoualmi-Zine. 2024. LLM-based edge intelligence: A comprehensive survey on architectures, applications, security and trustworthiness. *IEEE Open Journal of the Communications Society* (2024).

[63] Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador, and Narseo Vallina-Rodriguez. 2020. An analysis of pre-installed Android software. In *IEEE Symposium on Security and Privacy*. IEEE, 1039–1055.

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

[65] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. 2022. "Like lesbians walking the perimeter": Experiences of {US}.{LGBTQ+} folks with online security, safety, and privacy advice. In *31st USENIX Security Symposium*. 305–322.

[66] Alison Gemmill, Alexander M Franks, Selena Anjur-Dietrich, Amy Ozinsky, David Arbour, Elizabeth A Stuart, Eli Ben-Michael, Avi Feller, and Suzanne O Bell. 2025. US abortion bans and infant mortality. *JAMA* 333, 15 (2025), 1315–1323.

[67] Julia Gomula, Mark Warner, and Ann Blandford. 2024. Women's use of online health and social media resources to make sense of their polycystic ovary syndrome (PCOS) diagnosis: A qualitative study. *BMC Women's Health* 24, 1 (2024), 157.

[68] P Gowda and AN Gowda. 2024. Best practices in REST API design for enhanced scalability and security. *Journal of Artificial Intelligence, Machine Learning and Data Science* 2, 1 (2024), 827–830.

[69] Greg Guest, Arwen Bunce, and Laura Johnson. 2006. How many interviews are enough? An experiment with data saturation and variability. *Field Methods* 18, 1 (2006), 59–82.

[70] Marco Gutfleisch, Jan H Klemmer, Niklas Busch, Yasemin Acar, M Angela Sasse, and Sascha Fahl. 2022. How does usable security (not) end up in software products? Results from a qualitative interview study. In *IEEE Symposium on Security and Privacy*. IEEE, 893–910.

[71] Hana Habib, Megan Li, Ellie Young, and Lorrie Cranor. 2022. "Okay, whatever": An evaluation of cookie consent interfaces. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–27.

[72] Marian Harbach. 2024. Websites need your permission too–user sentiment and decision-making on Web permission prompts in Desktop Chrome. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–18.

[73] Shijing He, Yaxiong Lei, Xiao Zhan, Chi Zhang, Juan Ye, Ruba Abu-Salma, and Jose Such. 2025. Privacy perspectives and practices of Chinese smart home product teams. In *IEEE Symposium on Security and Privacy*.

[74] Natalie Hernandez, Alexander Trubowitz, and Sam Zacher. 2025. The insurance value of abortion and support for reproductive rights. *Political Behavior* (2025), 1–21.

[75] Jaap-Henk Hoepman. 2014. Privacy design strategies. In *IFIP International Information Security Conference*. Springer, 446–459.

[76] J-H Hoepman. 2018. Making privacy by design concrete. (2018).

[77] Sandra Höltervennhoff, Noah Wöhler, Arne Möhle, Marten Oltrogge, Yasemin Acar, Oliver Wiese, and Sascha Fahl. 2024. A {mixed-methods} study on user experiences and challenges of recovery codes for an {end-to-end} encrypted service. In *33rd USENIX Security Symposium*. 7267–7284.

[78] Minji Hong, Vasuki Rajaguru, KyungYi Kim, Suk-Yong Jang, and Sang Gyu Lee. 2024. Menstrual cycle management and period tracker app use in Millennial and Generation Z individuals: Mixed methods study. *Journal of Medical Internet Research* 26 (2024), e53146.

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

[80] Luke Hutton, Blaine A Price, Ryan Kelly, Ciaran McCormick, Arosha K Bandara, Tally Hatzakis, Maureen Meadows, Bashar Nuseibeh, et al. 2018. Assessing the privacy of mHealth apps for self-tracking: Heuristic evaluation approach. *JMIR mHealth and uHealth* 6, 10 (2018), e9217.

[81] Sarah J Iribarren, Kenrick Cato, Louise Falzon, and Patricia W Stone. 2017. What is the economic evidence for mHealth? A systematic review of economic evaluations of mHealth solutions. *PloS One* 12, 2 (2017), e0170581.

[82] Vijayanta Jain, Sepideh Ghanavati, Sai Teja Peddinti, and Collin McMillan. 2023. Towards fine-grained localization of privacy behaviors. In *IEEE 8th European Symposium on Security and Privacy*. IEEE, 258–277.

[83] Vijayanta Jain, Sanonda Datta Gupta, Sepideh Ghanavati, Sai Teja Peddinti, and Collin McMillan. 2022. Pact: Detecting and classifying privacy behavior of android applications. In *Proc. of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 104–118.

[84] Margaret Anne Johnson, Fiona Bloomer, and Gyða Margrét Pétursdóttir. 2025. "For some reason, she just wasn't able to have an abortion": Social attitudes, reproductive autonomy, and the taboo of regret. *Sex Roles* 91, 4 (2025), 32.

[85] Meg Leta Jones and Margot E Kaminski. 2020. An American's guide to the GDPR. *Denv. L. Rev.* 98 (2020), 93.

[86] JUSTIA. 1973. Roe v. Wade, 410 U.S. 113 (1973). https://supreme.justia.com/cases/federal/us/410/113/

[87] JUSTIA. 1992. Planned Parenthood of Southeastern Pa. v. Casey, 505 U.S. 833 (1992). https://supreme.justia.com/cases/federal/us/505/833/

[88] JUSTIA. 2022. Dobbs v. Jackson Women's Health Organization, 597 U.S. ___ (2022). https://supreme.justia.com/cases/federal/us/597/19-1392/

[89] Venkateswarlu Kajjam, Kakkerla Shivakumar, Sankoju Bhavani, M Satish Kumar, Sandi Sridhar Reddy, and Santhosh Kumar Medishetti. 2025. Preventing data leakage risks from DDoS and phishing attacks using random forest algorithm. In *4th International Conference on Innovative Mechanisms for Industry Applications*. IEEE, 1139–1146.

[90] Ina Kaleva, Alisa Frik, Lisa Mekioussa Malki, Mark Warner, and Ruba Abu-Salma. 2026. "I don't think it needs to be political": Privacy experiences and concerns of FemHealth app users in the United States. *Proc. on Privacy Enhancing Technologies* (2026).

[91] Risa Kaufman, Rebecca Brown, Catalina Martínez Coral, Jihan Jacob, Martin Onyango, and Katrine Thomasen. 2022. Global impacts of Dobbs v. Jackson Women's Health Organization and abortion regression in the United States. *Sexual and Reproductive Health Matters* 30, 1 (2022), 2135574.

[92] Harjot Kaur, Carson Powers, Ronald E Thompson III, Sascha Fahl, and Daniel Votipka. 2025. "Threat modeling is very formal, it's very technical, and also very hard to do correctly:" Investigating threat modeling practices in open-source software projects. In *USENIX Security Symposium*.

[93] Smirity Kaushik, Tanusree Sharma, Yaman Yu, Amna F Ali, Yang Wang, and Yixin Zou. 2024. Cross-country examination of people's experience with targeted advertising on social media. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. 1–10.

[94] Dilara Keküllüoğlu and Yasemin Acar. 2023. "We are a startup to the core": A qualitative interview study on the security and privacy development practices in Turkish software startups. In *IEEE Symposium on Security and Privacy*. IEEE, 2015–2031.

[95] Bridget G Kelly and Maniza Habib. 2023. Missed period? The significance of period-tracking applications in a post-Roe America. *Sexual and Reproductive Health Matters* 31, 4 (2023), 2238940.

[96] Abdullah Ayub Khan, Asif Ali Laghari, Roobaea Alroobaea, Abdullah M Baqasah, Majed Alsafyani, Rex Bacarra, and Jamil Abedalrahim Jamil Alsayaydeh. 2024. Secure remote sensing data with blockchain distributed ledger technology: A solution for smart cities. *IEEE Access* 12 (2024), 69383–69396.

[97] David A Klein, Scott L Paradise, and Rachel M Reeder. 2019. Amenorrhea: A systematic approach to diagnosis and management. *American Family Physician* 100, 1 (2019), 39–48.

[98] Jan H Klemmer, Marco Gutfleisch, Christian Stransky, Yasemin Acar, M Angela Sasse, and Sascha Fahl. 2023. "Make them change it every week!:" A qualitative exploration of online developer advice on usable and secure authentication. In *Proc. of the ACM SIGSAC Conference on Computer and Communications Security*. 2740–2754.

[99] Katie Krumbholz, Alice Militaru, and Kyle J Morgan. 2024. Tracking the trackers: 'Menstruapp' privacy policies following the Dobbs decision. *Journal of Women, Politics & Policy* (2024), 1–23.

[100] Ashutosh Kumar, L Kavisankar, S Venkatesan, Manish Kumar, Suneel Yadav, Sandeep Kumar Shukla, and Rahamatullah Khondoker. 2025. IoT device security audit tools: A comprehensive analysis and a layered architecture approach for addressing expanded security requirements. *International Journal of Information Security* 24, 1 (2025), 13.

[101] J Richard Landis and Gary G Koch. 1977. The measurement of observer agreement for categorical data. *Biometrics* (1977), 159–174.

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

[103] Hyunsoo Lee, Soowon Kang, and Uichin Lee. 2022. Understanding privacy risks and perceived benefits in open dataset collection for mobile affective computing. *Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 2 (2022), 1–26.

[104] Johanna Levy and Nuria Romo-Avilés. 2019. "A good little tool to get to know yourself a bit better": A qualitative study on users' experiences of app-supported menstrual tracking in Europe. *BMC Public Health* 19, 1 (2019), 1213.

[105] Karen EC Levy. 2014. Intimate surveillance. *Idaho L. Rev.* 51 (2014), 679.

[106] Tianshi Li, Yuvraj Agarwal, and Jason I Hong. 2018. Coconut: An IDE plugin for developing privacy-friendly apps. *Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (2018), 1–35.

[107] Jonathan Lord, Nicola Packer, Tonia Antoniazzi, Janet Barter, and Lesley Regan. 2025. Abortion law reform in the UK.

[108] Jonathan Lord and Lesley Regan. 2024. Triumphs and trials with the UK abortion law: The power of collaboration in abortion reform. *International Journal of Gynecology & Obstetrics* 164 (2024), 5–11.

[109] Isaac Maddow-Zimet and Candace Gibson. 2024. Despite bans, number of abortions in the United States increased in 2023. https://www.guttmacher.org/2024/03/despite-bans-number-abortions-united-states-increased-2023. Accessed: 2025-08-26.

[110] Shelly Makleff, Rebecca Wilkins, Hadassah Wachsmann, Deepesh Gupta, Muthoni Wachira, Wilson Bunde, Usha Radhakrishnan, Beniamino Cislaghi, and Sarah E Baum. 2019. Exploring stigma and social norms in women's abortion experiences and their expectations of care. *Sexual and Reproductive Health Matters* 27, 3 (2019), 50–64.

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

[112] Rohitha Sai Manne, Pramod Sai Gandla, Nikhil Shekhar Reddy, and Pokala Pranay Kumar. 2025. Patient data privacy and security in the healthcare industry. In *AI-Driven Breakthroughs in Antimicrobial Resistance*. IGI Global Scientific Publishing, 325–340.

[113] Hiroaki Masaki, Kengo Shibata, Shui Hoshino, Takahiro Ishihama, Nagayuki Saito, and Koji Yatani. 2020. Exploring nudge designs to help adolescent sns users avoid privacy and safety threats. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–11.

[114] Rowena Mason. 2025. Farage urged to explain anti-abortion links to meeting with Trump officials. https://www.theguardian.com/politics/2025/oct/16/farage-urged-to-explain-anti-abortion-links-to-meeting-with-trump-officials. Accessed: 2025-10-20.

[115] Joseph A Maxwell. 2010. Using numbers in qualitative research. *Qualitative Inquiry* 16, 6 (2010), 475–482.

[116] Nora McDonald and Nazanin Andalibi. 2023. "I did watch 'The Handmaid's Tale"': Threat modeling privacy post-roe in the United States. *ACM Transactions on Computer-Human Interaction* 30, 4 (2023), 1–34.

[117] Lula Mecinska, Carolyne James, and Kate Mukungu. 2024. Criminalization of women accessing abortion and enforced mobility within the European Union and the United Kingdom. In *Criminalizing Motherhood and Reproduction*. Routledge, 82–98.

[118] Maryam Mehrnezhad and Teresa Almeida. 2021. Caring for intimate data in fertility technologies. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–11.

[119] 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. In *Proc. of the European Symposium on Usable Security*. 1–14.

[120] Maryam Mehrnezhad, Thyla Van Der Merwe, and Michael Catt. 2024. Mind the FemTech gap: Regulation failings and exploitative systems. *Frontiers in the Internet of Things* 3 (2024), 1296599.

[121] Carlos M Mejía-Granda, José L Fernández-Alemán, Juan M Carrillo de Gea, and Jose A Garcia-Berna. 2025. A method and validation for auditing e-Health applications based on reusable software security requirements specifications. *International Journal of Medical Informatics* 194 (2025), 105699.

[122] Microsoft. 2025. Use end-to-end encryption for Microsoft Teams calls. https://support.microsoft.com/en-gb/office/use-end-to-end-encryption-for-microsoft-teams-calls-1274b4d2-b5c5-4b24-a376-606fa6728a90. Accessed: 2025-08-26.

[123] Lynn M Morgan. 2023. Global reproductive governance after Dobbs. *Current History* 122, 840 (2023), 22–28.

[124] Anton J Nederhof. 1985. Methods of coping with social desirability bias: A review. *European Journal of Social Psychology* 15, 3 (1985), 263–280.

[125] Nidhi Nellore, Tania Mishra, and Michael Zimmer. 2024. Unveiling user perspectives: Exploring themes in FemTech mobile app reviews for enhanced usability and privacy. *Proc. ACM Hum.-Comput. Interact.* 8, MHCI, Article 283 (Sept. 2024), 21 pages. https://doi.org/10.1145/3676530

[126] Sophie L Nelson. 2024. The post-Dobbs reality: Privacy expectations for period-tracking apps in criminal abortion prosecutions. *Pepp. L. Rev.* 51 (2024), 783.

[127] Ha-Nam Nguyen and Le Cuong. 2025. Overview of data classification and applications in data security. *International Journal of Environmental Sciences* (2025), 31–39.

[128] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[129] Nicolás Notario, Alberto Crespo, Yod-Samuel Martín, Jose M Del Alamo, Daniel Le Métayer, Thibaud Antignac, Antonio Kung, Inga Kroener, and David Wright. 2015. PRIPARE: Integrating privacy best practices into a privacy engineering methodology. In *IEEE Security and Privacy Workshops*. IEEE, 151–158.

[130] Phumezo Ntlatywa and Darelle van Greunen. 2024. A systematic literature review of usable privacy controls for mobile applications. In *International Conference on Intelligent and Innovative Computing Applications*. 116–126.

[131] Leysan Nurgalieva, Alisa Frik, and Gavin Doherty. 2023. A narrative review of factors affecting the implementation of privacy and security practices in software development. *Comput. Surveys* (2023).

[132] Aisling Ann O'Kane, Yvonne Rogers, and Ann E Blandford. 2015. Concealing or revealing mobile medical devices? Designing for onstage and offstage presentation. In *Proc. of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 1689–1698.

[133] Charlie Parker, Sam Scott, and Alistair Geddes. 2019. Snowball sampling. *SAGE Research Methods Foundations* (2019).

[134] Dilisha Patel, Ann Blandford, Mark Warner, Jill Shawe, and Judith Stephenson. 2019. "I feel like only half a man": Online forums as a resource for finding a "new normal" for men experiencing fertility issues. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–20.

[135] Uma Patel, Anna Broad, Rina Biswakarma, and Joyce C Harper. 2024. Experiences of users of period tracking apps: Which app, frequency of use, data input and output and attitudes. *Reproductive BioMedicine Online* 48, 3 (2024), 103599.

[136] Brennan Peterson, Orit Taubman-Ben-Ari, Bonnie Chiu, Douglas Brown, and David A Frederick. 2025. Infertility stigma and openness with others are related to depressive symptoms and meaning in life in men and women diagnosed with infertility. *Reproductive Health* 22, 1 (2025), 7.

[137] Shehani Pigera, Paul Van Schaik, Karen Renaud, Miglena Campbell, Petra Manley, and Pierre Esser. 2025. Privacy and security in digital health contact-tracing: A narrative review. *Applied Sciences* 15, 2 (2025), 865.

[138] Miloslava Plachkinova, Steven Andrés, and Samir Chatterjee. 2015. A taxonomy of mHealth apps–security and privacy concerns. In *48th Hawaii International Conference on System Sciences*. IEEE, 3187–3196.

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

[140] Aarathi Prasad, Jacob Sorber, Timothy Stablein, D Anthony, and David Kotz. 2014. Understanding user privacy preferences for mHealth data sharing. *mHealth Multidisciplinary Verticals* 30 (2014), 545–569.

[141] Maxwell Prybylo, Sara Haghighi, Sai Teja Peddinti, and Sepideh Ghanavati. 2024. Evaluating privacy perceptions, experience, and behavior of software development teams. In *20th Symposium on Usable Privacy and Security*. 101–120.

[142] Ravindra Putchakayala and Venkat Kishore Yarram. 2025. Adaptive trust engineering: AI-driven full-stack mechanisms for privacy, compliance, and data quality. *The Metascience* 3, 2 (2025), 1–21.

[143] Madeline Quasebarth, Madeleine Boesche, Tecora Turner, Amy Moore, Danielle Young, Debra Stulberg, and Lee Hasselbacher. 2024. Patient experiences using public and private insurance coverage for abortion in Illinois: Implementation successes and remaining gaps. *Perspectives on Sexual and Reproductive Health* 56, 3 (2024), 269–281.

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

[145] Daniel Reinhardt, Johannes Borchard, and Jörn Hurtienne. 2021. Visual interactive privacy policy: The better choice?. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–12.

[146] Grand View Research. 2023. Women's health app market size, share & trends analysis report by type (fitness & nutrition, pregnancy tracking & postpartum care, menopause), by modality, by region, and segment forecasts, 2025 - 2030. https://www.grandviewresearch.com/industry-analysis/womens-health-app-market. Accessed: 2025-08-26.

[147] Cedric Ryngaert and Mistale Taylor. 2020. The GDPR as global data protection regulation? (2020).

[148] Thwisha Sabloak, Isa Ryan, Skylar Nahi, Patrick Eucalitto, Melissa A Simon, and Ashish Premkumar. 2024. Intimate partner violence detected during abortion-related visits: A systematic review of screenings and interventions. *American Journal of Perinatology* 41, 12 (2024), 1697–1705.

[149] Kellen Safreed. 2019. Data protection law: The GDPR, CCPA, and US federal regulation. *REV. BANKING & FIN. L.* 39 (2019), 115–123.

[150] Shalini Saini and Nitesh Saxena. 2024. Privacy and security of women's reproductive health apps in a changing legal landscape. *arXiv preprint arXiv:2404.05876* (2024).

[151] Kowshik Sakinala. 2025. Monitoring and observability for cloud-native applications. *Journal of Computer Science and Technology Studies* 7, 8 (2025), 101–115.

[152] Gabrielle M Salvatore, Iris Bercovitz, and Danielle Arigo. 2024. Women's comfort with mobile applications for menstrual cycle self-monitoring following the overturning of Roe v. Wade. *MHealth* 10 (2024), 1.

[153] Karen Scarfone and Murugiah Souppaya. 2021. Data classification practices: Facilitating data-centric security management. (2021).

[154] Allysan Scatterday. 2021. This is no ovary-action: FemTech apps need stronger regulations to protect data and advance public health goals. *NCJL & Tech.* 23 (2021), 636.

[155] Juliane Schmüser, Philip Klostermeyer, Kay Friedrich, and Sascha Fahl. 2024. "I'm pretty expert and I still screw it up:" Qualitative insights into experiences and challenges of designing and implementing cryptographic library APIs. In *IEEE Symposium on Security and Privacy*. IEEE Computer Society.

[156] Farida Habib Semantha, Sami Azam, Kheng Cher Yeo, and Bharanidharan Shanmugam. 2020. A systematic literature review on privacy by design in the healthcare sector. *Electronics* 9, 3 (2020), 452.

[157] Bingyu Shen, Lili Wei, Chengcheng Xiang, Yudong Wu, Mingyao Shen, Yuanyuan Zhou, and Xinxin Jin. 2021. Can systems explain permissions better? Understanding users' misperceptions under smartphone runtime permission model. In *30th USENIX Security Symposium*. 751–768.

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

[159] Sheela Kakanur Shivayogi. 2025. Data classification methodologies and implementation. *Journal of Computer Science and Technology Studies* 7, 5 (2025), 202–210.

[160] Huzaifa Sidhpurwala, Garth Mollett, Emily Fox, Mark Bestavros, and Huamin Chen. 2025. Building trust: Foundations of security, safety, and transparency in AI. *AI Magazine* 46, 2 (2025), e70005.

[161] Baljeet Singh. 2025. Integrating threat modeling in DevSecOps for enhanced application security. *Available at SSRN* 5267976 (2025).

[162] Nakul Singh, Shreyas Kumar, Tripti Singh, and Pratyush Kumar. 2025. Building trust in smart TVs: AI-enhanced cybersecurity for user privacy and ethical monetization. In *European Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 647–655.

[163] Whitney Smith, Janet M Turan, Kari White, Kristi L Stringer, Anna Helova, Tina Simpson, and Kate Cockrill. 2016. Social norms and stigma regarding unintended pregnancy and pregnancy decisions: A qualitative study of young women in Alabama. *Perspectives on Sexual and Reproductive Health* 48, 2 (2016), 73–81.

[164] Daniel Smullen, Yuanyuan Feng, Shikun Aerin Zhang, and Norman Sadeh. 2020. The best of both worlds: Mitigating trade-offs between accuracy and user burden in capturing mobile app privacy preferences. *Proc. on Privacy Enhancing Technologies* (2020).

[165] Rebecca Smyth. 2024. Abortion in international human rights law: Missed opportunities in Manuela v El Salvador. *Feminist Legal Studies* 32, 1 (2024), 123–134.

[166] Society of Family Planning. 2024. #WeCount report: April 2022 to December 2023. Released: May 14, 2024. https://doi.org/10.46621/970371hxrbsk.

[167] Daniel J Solove. 2013. Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review* 126, 7 (2013), 1880–1903.

[168] Qiurong Song, Rie Helene Hernandez, Yubo Kou, and Xinning Gui. 2024. "Our users' privacy is paramount to us": A discourse analysis of how period and fertility tracking app companies address the Roe v Wade overturn. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–21.

[169] Qiurong Song, Renkai Ma, Yubo Kou, and Xinning Gui. 2024. Collective privacy sensemaking on social media about period and fertility tracking post Roe v. Wade. *Proc. of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–35.

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

[171] Karen Sowon and Wallace Chigona. 2020. Trust in mHealth: How do maternal health clients accept and use mHealth interventions?. In *Conference of the South African Institute of Computer Scientists and Information Technologists*. 189–197.

[172] Paul E Spector. 2019. Do not cross me: Optimizing the use of cross-sectional designs. *Journal of Business and Psychology* 34, 2 (2019), 125–137.

[173] State of Florida. 2023. Florida's 6-Week Abortion Ban (HB 7). https://www.flsenate.gov/Session/Bill/2023/7 Accessed: 2025-08-26.

[174] Athena Stavrou. 2025. Reform 'proudly embracing' anti-abortion politics as experts warn issue faces US-style politicisation in UK. https://www.independent.co.uk/news/uk/home-news/reform-anti-abortion-us-movement-farage-b2832865.html. Accessed: 2025-10-20.

[175] Hyewon Suh, Nina Shahriaree, Eric B Hekler, and Julie A Kientz. 2016. Developing and validating the user burden scale: A tool for assessing user burden in computing systems. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 3988–3999.

[176] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. 2023. Stuck in the permissions with you: Developer & end-user perspectives on app permissions & their privacy ramifications. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–24.

[177] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Deciding on personalized ads: Nudging developers about user privacy. In *17th Symposium on Usable Privacy and Security*. 573–596.

[178] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–15.

[179] Mohammad Tahaei, Marvin Ramokapane, Tianshi Li, Jason I Hong, and Awais Rashid. 2022. Charting app developers' journey through privacy regulation features in ad networks. In *The 22nd Privacy Enhancing Technologies Symposium*. De Gruyter Open Ltd., 33–56.

[180] Mohammad Tahaei and Kami Vaniea. 2019. A survey on developer-centred security. In *IEEE European Symposium on Security and Privacy Workshops*. IEEE, 129–138.

[181] Mohammad Tahaei and Kami Vaniea. 2021. "Developers are responsible": What ad networks tell developers about privacy. In *Extended Abstracts of CHI Conference on Human Factors in Computing Systems*. 1–11.

[182] Mohammad Tahaei, Kami Vaniea, and Awais Rashid. 2022. Embedding privacy into design through software developers: Challenges and solutions. *IEEE Security & Privacy* 21, 1 (2022), 49–57.

[183] Tahere Talebi Azadboni, Fahimeh Solat, Hanieh Hematti, and Meysam Rahmani. 2025. Information security and confidentiality in health chatbots: A scoping review and development of a conceptual model. *Digital Health* 11 (2025), 20552076251406637.

[184] Texas Legislature. 2021. Senate Bill 8, 87(R). https://capitol.texas.gov/BillLookup/History.aspx?LegSess=87R&Bill=SB8 Accessed: 2025-08-26.

[185] The National Archives. 1967. Abortion Act 1967. https://www.legislation.gov.uk/ukpga/1967/87/contents. Accessed: 2025-08-26.

[186] The White House. 2025. Fact sheet: President Donald J. Trump enforces overwhelmingly popular demand to stop taxpayer funding of abortion. https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-enforces-overwhelmingly-popular-demand-to-stop-taxpayer-funding-of-abortion/

[187] Nor Faiza Mohd Tohit and Mainul Haque. 2024. Forbidden conversations: A comprehensive exploration of taboos in sexual and reproductive health. *Cureus* 16, 8 (2024).

[188] Bel Trew. 2025. I gave birth three months early – then police investigated me over an illegal abortion. https://www.independent.co.uk/news/health/abortion-bill-vote-decriminalise-bpas-law-uk-b2771407.html. Accessed: 2025-08-26.

[189] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un) informed consent: Studying GDPR consent notices in the field. In *Proc. of the ACM SIGSAC Conference on Computer and Communications Security*. 973–990.

[190] Konstantina Vasileiou, Julie Barnett, Susan Thorpe, and Terry Young. 2018. Characterising and justifying sample size sufficiency in interview-based studies: Systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology* 18, 1 (2018), 148.

[191] Jocelyn Viterna and Jose Santos Guardado Bautista. 2017. Pregnancy and the 40-year prison sentence: How "abortion is murder" became institutionalized in the Salvadoran judicial system. *Health and Human Rights* 19, 1 (2017), 81.

[192] Maeve E Wallace, Charles Stoecker, Sydney Sauter, and Dovile Vilda. 2024. States' abortion laws associated with intimate partner violence–related homicide of women and girls in the US, 2014–20: Study examines the association of abortion laws to intimate partner violence of women and girls. *Health Affairs* 43, 5 (2024), 682–690.

[193] Mark Warner, Juan F Maestre, Jo Gibbs, Chia-Fang Chung, and Ann Blandford. 2019. Signal appropriation of explicit HIV status disclosure fields in sex-social apps used by gay and bisexual men. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–15.

[194] Lili Wei, Heqing Huang, Shing-Chi Cheung, and Kevin Li. 2025. How far are app secrets from being stolen? A case study on Android. *Empirical Software Engineering* 30, 3 (2025), 90.

[195] Maximiliane Windl, Albrecht Schmidt, and Sebastian S Feger. 2023. Investigating tangible privacy-preserving mechanisms for future smart homes. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–16.

[196] Ziang Xiao, Tiffany Wenting Li, Karrie Karahalios, and Hari Sundaram. 2023. Inform the uninformed: Improving online informed consent reading with an AI-powered Chatbot. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–17.

[197] Le Yu, Xiapu Luo, Xule Liu, and Tao Zhang. 2016. Can we trust the privacy policies of Android apps?. In *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. IEEE, 538–549.

[198] Nina Zadushlivy, Rizwana Biviji, and Karmen S Williams. 2025. Exploration of reproductive health apps' data privacy policies and the risks posed to users: Qualitative content analysis. *Journal of Medical Internet Research* 27 (2025), e51517.

[199] Razieh Nokhbeh Zaeem and K Suzanne Barber. 2020. The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems* 12, 1 (2020), 1–20.

[200] Haozhe Zhou, Mayank Goel, and Yuvraj Agarwal. 2024. Bring privacy to the table: Interactive negotiation for privacy settings of shared sensing devices. In *Proc. of the CHI Conference on Human Factors in Computing Systems*. 1–22.

[201] Sebastian Zimmeck, Peter Story, Daniel Smullen, Abhilasha Ravichander, Ziqi Wang, Joel Reidenberg, N Cameron Russell, and Norman Sadeh. 2019. Maps: Scaling privacy compliance analysis to a million apps. *Proc. on Privacy Enhancing Technologies* (2019).

[202] Verena Zimmermann. 2023. Privacy nudges and informed consent? Challenges for privacy nudge design. In *Human Factors in Privacy Research*. Springer International Publishing Cham, 155–171.

[203] Wenxue Zou, Lu Tang, and Cara Wallis. 2025. "My body is betraying me": Exploring the stigma and coping strategies for infertility among women across ethnic and racial groups. *Health Communication* (2025), 1–12.