Collective Privacy Sensemaking on Social Media about Period and Fertility Tracking post Roe v. Wade

QIURONG SONG, The Pennsylvania State University, USA
RENKAI MA, The Pennsylvania State University, USA
YUBO KOU, The Pennsylvania State University, USA
XINNING GUI, The Pennsylvania State University, USA

On June 24, 2022, the U.S. Supreme Court overturned Roe v. Wade, which has led to full bans on most abortions in 14 states within one year. Many people in the U.S. use period and fertility tracking apps for reproductive healthcare and concerns have arisen about the privacy risks these apps might pose in the wake of Roe reversal. Existing literature on privacy risks of period and fertility tracking apps has primarily examined the privacy policies and practices of these apps. However, how users make sense of the privacy risks of these apps, especially in the post-Roe time, remains understudied. This study explores collective privacy sensemaking on social media, a practice in which people collectively make sense of a privacy situation. Our findings reveal how people contextualize privacy issues, speculate about the associated risks, as well as explore risk mitigation strategies. We conclude with privacy design implications for privacy design in period and fertility tracking apps and contribute insights that could inform policymaking and legal perspectives.

CCS Concepts: • **Human-centered computing → Collaborative and social computing → Empirical studies in collaborative and social computing;** • **Human-centered computing → Human computer interaction (HCI) → Empirical studies in HCI.**

Additional Key Words and Phrases: Period tracking, fertility tracking, personal informatics, reproductive health, privacy risk, collective privacy sensemaking, risk assessment, risk mitigation, social media, overturn of Roe v. Wade, post-Dobbs

ACM Reference Format:
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. ACM Hum.-Comput. Interact.,*** 8, CSCW1, Article 161 (April 2024), 35 pages, https://doi.org/10.1145/3641000

1 INTRODUCTION

On June 24, 2022, the Supreme Court in the United States overturned a nearly 50-year precedent in Roe v. Wade, essentially giving states the license to ban abortion. This has led to full bans on most abortions in 14 states and stricter restrictions on reproductive rights in others [97,158]. Soon

Authors' addresses: Qiurong Song (qiurongsong@psu.edu), Renkai Ma (renkai@psu.edu), Yubo Kou (yubokou@psu.edu), and Xinning Gui (xinninggui@psu.edu), College of Information Sciences and Technology, The Pennsylvania State University, State College, PA, USA.

2573-0142/2024/4 - 161

https://doi.org/10.1145/3641000

after the ruling was announced, an online call to delete period and fertility tracking apps quickly aroused [63]. Period and fertility tracking often overlap in functionality. Period tracking mostly monitors menstrual cycles and predicts menstrual dates [169], while fertility tracking mostly predicts ovulation and fertile windows [5]. Both types require similar user inputs like period start and end dates, mood, and sexual activity. Popular apps like Flo encompass both functionalities. In this paper, we collectively refer to them as "period and fertility tracking apps." In the U.S., nearly one-third of women have used these apps to track their menstrual cycle [96]. Users' menstrual information collected by period and fertility tracking apps could be used as digital evidence against pregnant people and providers in prosecutions of abortion [33,34]. After the overturn of Roe v. Wade, these tracking apps suddenly present a tangible risk to their users.

Previous research in HCI has examined the privacy issues of period and fertility tracking apps [4,53,60,79,110,143], focusing on their privacy policies [60,143] and practices [53,111]. Researchers found that most apps lack appropriate measures to deal with intimate health data, merely treating it as a special category of data, and some apps even share user data with third parties [53,60,110,143]. Many period and fertility tracking apps fail to provide users with adequate, transparent information on data privacy, making it difficult for users to understand the implications of sharing sensitive data with the apps [111,143]. With the overturn of Roe v. Wade, the present privacy practices of these apps pose greater risks, potentially leading to prosecutions over illegal abortions [34], or harassment against people regardless of whether they get abortions legally [109]. However, a limited number of studies have investigated users' privacy concerns about period and fertility tracking apps. A notable exception revealed that many users experienced an escalation of privacy risks and thus deleted period and fertility tracking apps to mitigate these risks [108].

In addition, previous scholarship tends to focus on the scales of the individual and the group, revealing individual or group-based perspectives and collaborative privacy management [18,26,45,89,99]. However, the privacy risks associated with the overturn of Roe v. Wade affect an entire demographic—women and people with uteruses. The overturn of Roe is a societal issue and poses significant challenges to privacy in period and fertility tracking, introducing additional legal-related risks and complexities. Therefore, it is important to go beyond individual concerns and understand how people collectively make sense of the privacy risks and consider the broader societal implications and perspectives. Sensemaking refers to "placement of items into frameworks, comprehending, redressing surprise, constructing meaning, interacting in pursuit of mutual understanding, and patterning" [166], and has been used as a productive lens in CSCW (e.g., [59,100,171]). Collective privacy sensemaking, then, denotes the practices of people working together to develop a mutual understanding of a privacy situation, which is the overturn of Roe v. Wade in this study. This study seeks to draw from the lens of collective sensemaking to uncover users' privacy perception and risk assessment.

In this paper, we seek to fill the research gap by exploring the following research question: how users collectively make sense of privacy in period and fertility tracking. Specifically, we collected and qualitatively analyzed discussions on Reddit about people's experience of period and fertility tracking apps after the overturn of Roe v. Wade, leading to a detailed depiction of collective privacy sensemaking about privacy of period and fertility tracking. We found that people collectively assess data privacy of period and fertility tracking apps with contextual information, such as app companies' official documents, historical actions, and business models. People also speculate about the privacy risks that the overturn of Roe might induce or intensify, such as the risks of prosecution, surveillance and harassment. Perceiving the privacy risks, people

brainstorm strategies to resist possible data surveillance and collaboratively protect their privacy. We concluded with implications for period and fertility tracking app design and policy making.

Our contributions are three-fold: First, our detailed analysis of privacy sensemaking and coping strategies in period and fertility tracking from the user perspective contributes to the current literature on people's privacy perception and data practice of using period and fertility tracking apps. Second, our work provides empirical and conceptual insights into people's collective sensemaking of complex, societal level privacy risks. Third, we not only derive implications for future privacy design of period and fertility tracking apps, but also contribute insights to policy making and legal perspectives.

2 BACKGROUND

In 1973, the U.S. Supreme Court's landmark Roe v. Wade decision recognized a constitutional right to abortion under the "right to privacy," decriminalizing it nationwide [159]. After this decision, people had the right to have abortions legally across the country, and patients were able to get the reproductive healthcare they needed, without fear, when they needed it. However, on May 2, 2022, a leaked draft revealed the potential overturning of Roe v. Wade [65]. This became a reality on June 24, 2022, when a slim majority of the Court overturned a nearly 50-year precedent in Roe v. Wade and gave states the license to ban abortion. As of June 2023, the overturn has led to full bans on most abortions in 14 states and stricter restrictions over reproductive rights in others [97,158]. The decision was met with both celebration and anger, setting off protests and rallies across the country [82,107].

Soon after the ruling was announced, an online call to action quickly aroused: Delete your period tracking app. The call began in May 2022 when the draft supreme court opinion indicating the overturn of Roe v. Wade was leaked, and has intensified since the Court officially revoked it [63]. Period and fertility tracking constitute a major part of the growing "Femtech" industry.[1] Femtech denotes a category of technology innovations "such as temperature patches, insertable devices, wristbands, clip-ons, smart jewelry, DNA testing related to fertility and many other devices and data analytics helping people figure out their female health" [160]. The femtech market is estimated to reach a value of $50 billion by 2025 [154]. As a major part of the femtech industry, period and fertility tracking apps are used by many women and people with uteruses to track their periods and obtain predications for future cycles [160]. In the United States, nearly one-third of women have used these apps to track their menstrual cycle according to a 2019 survey [96]. Women and people with uteruses using these apps were suddenly fearful that their collected data could be used against them post Roe.

These concerns are not unfounded. Period and fertility tracking apps collect detailed sensitive reproductive health information [28,57]. When combined with personal data, this information can potentially be used as digital evidence in abortion-related legal cases [33,34]. For example, in 2017, a Mississippi prosecutor indicted a woman for second degree murder after a stillbirth, pointing out that her Internet search history mentioned misoprostol [130,172]. The overturn of Roe v. Wade would significantly impact healthcare, notably abortion care and women's reproductive healthcare [19,29,31,56,91,93,161]. The clash between politics and reproductive healthcare may increase challenges to personal health management and have potential mental health implications [19,29]. The overturn of Roe v. Wade could also resonate globally [29,67,81,91,145]. Negative impacts on abortion laws and policies may occur in different ways,

[1] We recognize the label "Femtech" is problematic, as it excludes transgender and nonbinary people [66].

such as slowing the worldwide trend toward liberalization of abortion laws and increasing the prosecution of people who seek or provide abortions in violation of legal criteria [81,145].

3 RELATED WORK

3.1 Period and Fertility Tracking and Their Privacy Issues in HCI and CSCW

Women and people with uteruses across different life stages track their menstrual cycle for varied reasons. For instance, period and fertility self-tracking provides a sense of agency, facilitates informed discussions with healthcare providers, and supports personalized care, playing a crucial role in helping individuals manage complex health conditions [36,37,162]. Such tracking is not only related to health management, but also has social connotations [6]. HCI research emphasizes the cultural and societal influences on tracking designs [6,23,80,148]. In some societies, menstruation self-tracking is closely related to self-identity and emancipation [80,162]. However, current design often ignores the social, cultural, and political influences on women's health [148].

Privacy issues associated with period and fertility tracking have also been a focal point in the fields of HCI and CSCW. Extensive research has examined the privacy practices that these apps officially disclosed in their documentation, utilizing methods such as app review and policy analysis [4,46,53,60,110,143]. Many apps share user data with third parties and fail to follow existing data protection regulations, such as General Data Protection Regulation (GDPR) [4,53,143], which raises privacy and security concerns, including potential user surveillance [60]. Moreover, privacy policies of these apps often lack effective information and transparency, making it difficult for users to understand the implications of sharing sensitive data and to exercise their rights [60,143]. Specifically, while most apps appropriately displayed their practices regarding personal data such as names and email addresses, they failed to make clear or even mention their handling of reproduction-related data in their privacy policies [143]. Alarmingly, the disclosed privacy measures of these apps might not reflect their true data handling procedures, with some displaying concerning lapses such as inadequate data encryption [53,110]

While extensive studies focused on privacy practices of these apps, only a few have examined users' actual privacy concerns. Findings from two interview studies indicated users were not very concerned about their period tracking data privacy [79,102]. They viewed their period and fertility tracking data as "not that personal" and "uninteresting for anyone beyond themselves." Yet, following the overturn of Roe v. Wade, privacy concerns have intensified, leading many to delete period tracking apps, even though they had hardly changed their privacy strategies of using other technologies [108]. However, there still remains a lack of understanding regarding how individuals perceive and make sense of the privacy risks associated with these apps.

In sum, prior HCI and CSCW studies have delved into the practices of period and fertility tracking apps and highlighted their shortcomings [4,53,60,110,143]. Besides, they touched upon users' privacy concerns and risk handling approaches of these apps [46,79,108]. However, a deeper and more focused investigation into users' privacy sensemaking of using period and fertility tracking apps is needed, especially in this post Roe time. Our study aims to bridge this gap, exploring collective navigation of privacy challenges of these apps in the wake of Roe v. Wade's overturn.

3.2 Privacy Issues on Period and Fertility Tracking Apps through a Legal Perspective

In addition to HCI and CSCW scholars, legal scholars have also started paying attention to the privacy issues of period and fertility tracking apps. Their research resonates with HCI studies,

pointing out the inadequacy of privacy measures and the resulting data privacy risks in these apps [104,135], especially in the US context [135]. Although the Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects against unauthorized disclosure of sensitive patient health data, period and fertility tracking apps often fall outside its purview [25,135]. California has recently strengthened protections for reproductive health data, but to date, there is no comprehensive federal digital privacy legislation in the US [149,152]. With weak privacy regulations, sensitive health data in period and fertility tracking apps is vulnerable to misuse, including leading to workplace biases [22]. The overturn of Roe v. Wade has intensified these privacy risks as new abortion restrictions may even clash with current health privacy protections [113,149].

Outside the US, a few data protection regulations have come into effect including GDPR, which is considered one of the toughest and most accurate privacy laws in the world [133,168]. GDPR recognizes “data concerning health” as a “special category of data” and gives them extra protection [54,84]. However, for reproductive health data, including fertility data, there are currently no specific data protection regulations outside of health and medical clinics [84,110]. This ambiguity and unclearness in the law can pose risks to those who use technologies such as period and fertility tracking apps [110,167].

In sum, previous studies have focused on the inadequacy of privacy regulations on period and fertility tracking apps and associated risks to app users [38,110,113,135,149]. However, there is limited understanding of how users understand and react to the current legal status of privacy protection of their period and fertility data. Incorporating users' perspectives by examining how users navigate the current legal landscape provides a more comprehensive understanding of privacy issues of period and fertility tracking. In this way, we aim to inform policy design at both the app and governmental levels, and also contribute to HCI and CSCW areas with actionable policy-informed design guidelines to protect user privacy.

3.3 Risk Assessment and Privacy in Context

Risk assessment is an overall process of risk analysis and evaluation, which identifies possible hazards, their likelihoods and consequences, and the tolerance for such events based on risk analysis [16,131]. Risk assessment can be at the individual or broader system level [16,78,131]. At the individual level, risk assessment may not always follow a purely economic rational process. Factors beyond strict probabilities calculations, including the assessor’s personal biases and experiences, influence their decision making [78,151]. Individuals employ a range of risk mitigation strategies to both prepare for and lessen the impact of potential hazards [42,61].

In terms of privacy risks on a broader system scale, past studies have offered multiple frameworks for experts to systematically handle risk assessment in areas like healthcare and cybersecurity [3,14,44,90,165]. At the individual level, privacy risk assessment is contextual and influenced by the individual's intent or purpose for sharing information. The contextual integrity theory indicates privacy adheres to specific "norms" shaped by societal factors [120,121]. In mobile app usage, aligning information disclosure with these norms can be challenging for users [121,144]. Thus clear communication about privacy risks, such as using personalized examples, can better guide users [8,74,87].

Building upon existing research on privacy risk assessment and mitigation, our work aims to expand these research strands by investigating from a user perspective and focusing on how users collectively assess privacy risks in using period and fertility tracking apps.

3.4 Privacy Beyond the Individual and Collective Sensemaking

As contextual integrity theory indicates, privacy is not solely an individual concern, but is inherently interconnected and interdependent in the context of society [120], which acknowledges the collaborative nature of privacy protection. Previous research has introduced different terms, such as collective privacy management and collaborative privacy management to conceptualize such collective process of privacy management [89,150]. However, most studies primarily focus on assisting individuals within a group in making disclosure decisions, rather than addressing the privacy protection for the group as a whole [153].

Another relevant concept is group privacy, which entails protecting the privacy rights of both individual group members and the group as a collective entity [58,153]. It extends the concept of individual privacy and addresses potential privacy threats arising from big data analytics [58,153,157]. The term "group" encompasses both socially-determined groups, which are recognized and acknowledged by society, and algorithmically-determined groups based on shared characteristics or behaviors [153]. Group privacy involves protecting groups from harms from data inferences and profiling [58,153,156]. Group privacy protection necessitates understanding both individual and collective privacy rights, calling for new approaches that acknowledge the autonomy of groups [27,88,153].

The discussion of people perceiving, contextualizing and assessing privacy on both individual and group levels can be viewed as the process of collective sensemaking. Sensemaking is a social activity through which individuals and groups create meaning and understanding in ambiguous or complex situations [21,166]. It involves actively interpreting and organizing information from the surroundings to make sense of personal experiences, reduce uncertainty, and guide action in dynamic environments [40,166]. Sensemaking is influenced by collective interactions and shared contexts, shaping both individual and group understanding [21,86,166]. Many previous studies in CSCW have adopted the framework to examine the collective sensemaking in online discussions facilitated by social media [43,100].

Building upon existing research on privacy risk assessment and collective sensemaking, our work aims to expand these research strands by investigating from a user perspective and focusing on how users collectively make sense of the privacy in using period and fertility tracking apps.

4 METHODS

4.1 Data Collection

We collected and analyzed social media data to investigate people's collective sensemaking of privacy issues on period and fertility tracking apps post-Roe. It is a common practice in HCI and CSCW to use social media data for research on sensitive topics [10,11,72,124]. Besides, social media platforms are ideal for studying collective sensemaking due to their discussion-fostering nature. Numerous CSCW and HCI studies have used social media, including Reddit, for such research (e.g., [100,101,106]). After evaluating multiple social media platforms including Twitter, Facebook, and Reddit, we opted for Reddit. Twitter's brevity limited the depth of insights for sensemaking process, while Facebook's identity-linked nature could deter open discussions on stigmatized topics like reproductive health [9,73,163]. As one of the most popular and largest online digital destinations with over 52 million daily active users [132], Reddit offers both a vast dataset and a relatively safe platform for discussing the sensitive topic.

We did not focus on any specific subreddits for data collection due to the political nature of abortion-related discussion and it would be biased to focus only on specific subreddits [146] such

as “Political_Revolution” and “AskThe_Donald” which have strong political leanings. For data extraction, we utilized Python packages, PRAW and PMAW, accessing Reddit's API to retrieve threads and comments with relevant keywords. We searched keywords primarily on thread content and titles, excluding search in comments because the data with keywords appearing in thread content often contains more focused discussion.

We conducted data collection in four steps. First, we generated a preliminary list of keywords derived from literature on period and fertility tracking (e.g., [23,52,118,135,162]) and relevant media reports (e.g., [63,116,136]). In the end, the initial keywords included {cycle tracking, period tracking, fertility tracking, menstruation tracking, menstruation app}. We also added all the variations of each keyword (e.g., the word "track" has variations such as tracker and tracking) to ensure the completeness of the search results. We excluded "Roe v. Wade" to avoid retrieving numerous irrelevant posts. Second, after the initial search, we reviewed around 30 threads to refine our keyword list. This step helped to include more contextual and spoken keywords that people often used in these discussions, through which we identified some additional keywords, including {menstrual cycle tracking, Flo app, Clue app}. The final keyword set we used was {cycle tracking, period tracking, menstruation tracking, menstruation app, menstrual cycle tracking, fertility tracking, Flo app, Clue app} and their variations. Third, we collected content and comments of threads that mentioned any of these keywords posted from June 24, 2022 to October 2, 2022. Initially, our search started from May 2, 2022—the date a leaked Supreme Court decision hinted at the overturning of Roe v. Wade [65]. However, due to limited relevant discussions between May 2 and June 24 (the official overturn date), we focused on the latter timeframe. Our final retrieved dataset was the threads posted from June 24, 2022 to October 2, 2022, and their comments. Fourth, after removing duplicates, we obtained a dataset containing 1,743 threads associated with 22,592 individual comments. The appendix lists the subreddits where the posts we collected were published.

4.2 Data Analysis

We first analyzed the trend in the number of daily posts on period and fertility tracking post Roe to decide which posts we would start our data analysis with first. 26.4% of threads were posted in the week after the decision, with most of the threads related to post-Roe period and fertility tracking. Figure 1 depicts a decreasing trend in such posts over time, indicating decreased discussions on this topic as time progresses. We also noticed that some threads were informative and received a lot of likes, but few comments. Therefore, we did not use comment count as a filtering criterion.

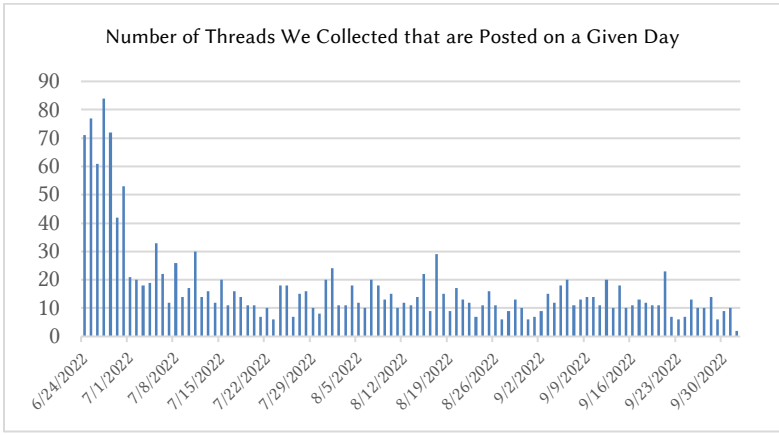

Fig. 1. Daily trend of posts related to period and fertility tracking from June 24, 2022, to October 2, 2022.

We conducted an inductive thematic analysis to analyze our Reddit dataset [20], involving a team of four researchers. Initially, each of us individually read the data to familiarize ourselves with it. Among the 1,743 Reddit posts, we first selected the first 200 posts published that are relevant to period and fertility tracking after the time Roe v. Wade was officially overturned, and these posts were published between June 24 to June 26. We also added random threads from later dates to capture evolving insights. Subsequently, we independently assigned initial codes to segments of the data that represent distinct concepts. During the process, we continuously compared new data with previously reviewed data and codes we have developed to identify new concepts and refine existing ones. Concurrently, we had regular weekly meetings to discuss the initial codes, which helped to settle disagreements and combine the initial codes. We continued this process and consistently assessed whether new data is providing additional insights. We agreed that we reached "theoretical saturation" when new data no longer brought up new concepts or insights, and our established codes comprehensively captured all facets of the data [35]. In the end, we coded a total of 311 threads and their associated 5302 individual comments. During the process, we gave each data item adequate and equal attention and coded for as many potential themes as possible [20], which led to 399 initial codes. After this, we met several times to discuss the combination of similar initial codes to generate higher-level themes. During the process, we moved back and forth between codes and data to refine the themes, aiming for "internal homogeneity and external heterogeneity" [125]. Our final thematic scheme includes three primary themes: contextualizing data privacy, speculating about privacy risks, and resisting data surveillance.

When reporting our findings, we used U1, U2, etc. to indicate the different users on Reddit. This study is part of a project which was approved by IRB from the university. The study itself was approved for exemption by the IRB since it did not involve human subjects. Previous research has highlighted ethical challenges in using data from social media platforms such as Reddit [128,164], including concerns about privacy, user anonymity, and data discoverability. In light of these issues, our study approached the collection and presentation of Reddit data with great care. The data we collected do not contain personally identifiable information. Considering Reddit is open to the public, to further protect Redditors' privacy, we reduced the data's searchability by rewording the quotes while maintaining their original meaning.

4.3 Researcher Positionality and Reflexivity

In this subsection, we articulate our positionality, sense of self, and personal experiences that have shaped our research inquiry [51,129]. The first and last authors are cis gender females. The second and third authors are cis gender males. The last author herself is a long-time period tracking user, who shares some similar lived experiences and concerns with those that surfaced in our study. In addition, the last author considers herself as a feminist, and has done research on maternal health and reproductive rights in the past. Thus, she can be considered as having "insider" perspectives. However, as many scholars have argued, the outsider-insider distinction is a false dichotomy as both so-called outsiders and insiders need to contend with methodological considerations around positionality [129]. Moreover, the false divide between "insider" and "outsider" research actually risks controlling "who felt entitled to speak out and who could be trusted to hear" [115]. We acknowledge that the last author's personal engagement with period tracking and interests in maternal health and reproductive rights motivated and informed the research. However, all of us strive for objectivity even though pure objectivity is an unattainable, idealized goal as "the subjective and objective components of knowledge are interconnected and interactive" [17]. Specifically, we strived to achieve "empathic neutrality" [126] during the whole study process to avoid possible biases and to be as neutral as possible in the data collection, interpretation, and presentation. For instance, as we detailed in the data collection subsection, we searched Reddit sitewide instead of focusing on specific subreddits to mitigate possible biases. Also, when analysing the data, we followed thematic analysis to analyse the data mindfully, rigorously, and inductively, focusing on understanding and interpreting the data authentically while avoiding judgments or using any predefined theories/framework to guide the data analysis.

5 FINDINGS

The post Roe v. Wade discussions on Reddit supported concerned citizens' collective sensemaking centered on the overturn's profound implications on data privacy of end users of period and tracking apps. While previous studies have primarily focused on privacy decision-making on individual or group level [45,89,150,153], our findings revealed community-level privacy sensemaking via social media. Specifically, their collective sensemaking had three interconnected strands: contextualizing data privacy, speculating about privacy risk, and resisting data surveillance.

5.1 Contextualizing Data Privacy

The overturn prompted Reddit users to collectively explore each period and fertility tracking app's specific privacy conditions. In doing so, the collective sensemaking put the issue of data privacy in context, rather than following a one-size-fits-all understanding. While contextual integrity theory mostly emphasized the societal factors in individuals' privacy decision making [120,121], our data further revealed how individuals collectively assess contextual factors to make sense of the privacy risks as a community.

5.1.1 Contextualizing privacy in companies' documents after Roe v. Wade

A company's official documents, such as terms of service (TOS), privacy policy and statements addressing the overturn of Roe, provide significant contextual information for users to assess the data privacy of this app. People typically refer to these documents to assess an app's data handling. When contextualizing privacy in companies' responses, users not only considered the

content but also the language clarity and sincerity. For instance, a user expressed their disappointment in an app (Flo) after reading its statement,

> U3: I actually deleted the app after receiving that email. It seemed hollow, insincere, and way too ambiguous to trust.

The user was disappointed and deleted the Flo app after reading its statement because they felt it was not clear and trustworthy. When assessing privacy in the context of an app's claimed practices, people tried to not only understand the literal meaning of the language in their official documents, but also decipher the hidden views or attitudes of the app companies.

Updating documents such as privacy policy and TOS is a normal practice for app companies to reflect changes in their practices and comply with new regulations. Contextual factors such as timing of the changes and what changes they made greatly affect people's privacy assessment. For example, here is a discussion excerpt on Stardust app's statement,

> U4: Stardust said that it updated its policy; it now says it will "comply with or respond to law enforcement or a legal process or a request for cooperation by a government or other entity, when legally required (…)" I still don't trust them.
> U5: In addition, the updated statement has a legal loophole of the word OR. "Comply with OR respond" Or etc. It's literally a vague enough opening in verbiage to just hand over data without drama.
> U4: (…) the vague language and the fact that they changed it only after they were called out on it. (…)

U5 pointed out the legal loophole in the updated statement, which they believed introduced ambiguity and potentially allowed the app to hand over user data without facing any consequences. U4 noted the app's timing of policy changes, which suggested that the update was a reactive measure rather than a proactive commitment to privacy. The contextual information regarding the app's policy changes undermined the perceived sincerity of the app's privacy practices.

5.1.2 Contextualizing privacy in companies' historical actions

Historical actions, or what a company did in the past about user data, are informative in people's trust in app companies and assessment of data privacy. In evaluating a company's claimed and actual privacy practices, users interpreted and decided whether to trust a company's statements based on its historical actions. For example, a thread discussed a statement email from Flo app addressing the Roe v. Wade overturn,

> U3: Thought people here might be interested in this update (…) "Dear Flo community, in light of Roe v. Wade being recently overturned (…) If Flo were to receive an official request to identify a user by name or email, Anonymous Mode would prevent us from being able to connect data to an individual, meaning we wouldn't be able to satisfy the request (…) your data remains safe and secure with Flo. Our users' health data will never be shared with any company but Flo (…)"
> U6: This statement seems untruthful or insincere, since they just settled last year with the Federal Trade Commission about sharing personal data with third parties. Data privacy is at the core of their operations? Since uh, we got busted for it? (…)
> U7: Indeed. I received this email from Flo because my own personal data had been shared by it:

> "Dear Flo User, Between June 30, 2016, and February 23, 2019, the company that makes the Flo Period & Ovulation Tracker app sent an identifying number related to you and information about your period and pregnancy to companies that help us measure and analyze trends, usage, and activities on the app, including the analytics divisions of Facebook, Flurry, Fabric, and Google (…)"

U3 shared Flo's statement, which promised that user data are secure and will never be shared with other companies. However, many people still cast doubt on the safety of Flo when they put the company's data privacy practice in its historical context. These users pointed out this period tracking app has a history of sharing intimate data regarding period and pregnancy with government. They did not have control over their own data and were only notified by Flo after their data had been shared. Consequently, although Flo's statement emphasized that user data was safe with them after the overturn of Roe, people found this hard to believe. The stark contrast between the company's historical actions and its statement raised suspicions about the trustworthiness of its declaration.

In the similar vein, people were likely to trust an app if it has a history of valuing user privacy. For example, a user expressed their trust in Apple health,

> U8: Despite Apple, like all large companies, has a long bloody list of violations against society, which I am not excusing. But its stance on privacy and encryption all the way down to the "bare metal" is very clear.

The user pointed out that Apple had a consistent stance on privacy protection and was known for its encryption technology. Thus, in a context where it has consistently valued user privacy in the past, the user indicated that using Apple Health to track period and fertility might be a safe option.

5.1.3 Contextualizing privacy in companies' respective business model

The business model of period and fertility tracking apps is also a major contextual factor in how people assess the privacy of their data on these apps. Business model refers to the framework or structure that an organization uses to create and deliver value [173]. A company's framework for creating value, including profiting strategies can affect how it makes use of user data. Therefore, many people evaluated the apps' business models to assess their privacy practices. For example, a user wrote,

> U9: (…) If a product is FREE, YOU ARE THE PRODUCT BEING SOLD. That goes for every other free mobile app I've ever heard of!

The user argued that free digital products generally tend to use user data to make a profit which might violate users' privacy simultaneously. Thus, when it came to a free period and fertility tracking app, the user feared that it would also sell their health data for profits, leading to their distrust in these apps.

People also reasoned about a company's business model to estimate whether it would take the risk of selling user data to make a profit. For example, a user shared their privacy assessment,

> U8: For Apple, selling your data is completely worthless compared to the revenue generated from Apple's hardware sales - all the effort just to cover up your suggested level of data infringement would be a massive risk for little gain (…)

This user believed that Apple's massive hardware sales revenue diminishes any incentive to profit from user data. In addition, they perceived that the effort required to cover up any potential

privacy violations and the associated risks are significant and outweigh any potential benefits for Apple. By evaluating its business model and its potential emphasis on user privacy, the user contextualized Apple Health's privacy, leading them to have confidence in their data safety.

Users tended to believe that an application is safer in terms of privacy if it does not or cannot profit from user data. For example, a user wrote,

> U10: If I needed something like that (a named tracking app), I personally would try to find an open-source offline app. Maybe it won't be as pretty and user friendly as the other apps, but at least I could trust it.

An offline open-source app generally does not have the inherent capability to share user data due to its lack of direct internet access. The user believed that an open-source offline app is more reliable and trustworthy in privacy than other apps as its business model usually prioritizes transparency and limits the app's ability to collect and share user data.

People worried about big tech companies monetizing their data see non-digital tracking as a privacy safeguard. For example, a user wrote,

> U11: I still have a paper calendar on the fridge. Paper isn't obsolete, and google/amazon/Microsoft/apple/etc. have no access to it.

The user shared their practice of using a non-digital approach to track menstruation and proactively advocated for its benefits of both preserving personal health data and protecting privacy. Large technology companies are often perceived as potentially profiting from or sharing user data. In this context, this user believed that a non-digital approach would protect their privacy by making their data inaccessible to these companies.

5.1.4 Contextualizing privacy in companies' locations

An app company's location affects the privacy laws and regulations to which the company is subject. Privacy laws vary from country to country and, therefore, many considered the location of the app company as an important contextual factor in evaluating its data privacy. In addition, people paid attention to the locations of third-party collaborators linked with these apps, such as those handling data storage or processing. For instance, while some trusted Clue because it is based in the EU and adheres to strict privacy laws, others expressed skepticism,

> U13: A European company may be hosting data outside the EU, making it subject to different legal frameworks and cross-border agreements (…) Clue's statement doesn't speak for the third-party companies storing the data…

This user noticed that it was unclear if Clue has third-party collaborators located outside the EU that may be subject to different privacy regulations. In this example, the user considered the specific legal framework that third parties who may have access to the user's data must comply with, and assessed data privacy accordingly.

However, people emphasized the need to evaluate not just an app company's location but also its potential response to legal requests. Despite stringent local privacy laws, vulnerabilities can remain. For example, a user argued,

> U13: The fact that GDPR applies is not that relevant in this case. When it comes to a legitimate legal request from U.S. authorities, European companies usually comply.

Federal statutes and regulations apply to U.S. companies and foreign companies with a presence in the U.S. This user pointed out that even if a company is located in the EU, that does

not guarantee it is legally risk-free. People used location as a contextual factor when evaluating an app's privacy, but they also considered other factors, such as specific legal practices under cross-country data requests, and evaluated them together.

5.2 Speculating about Privacy-Related Risks

Although these discussions on Reddit took place right after the overturn when nothing had happened yet, Reddit users were quick to make inferences in terms of how such overturn would induce or intensify the privacy risk of period and fertility tracking, as well as the potential risks that could arise from privacy violations. While previous research on risk assessment mostly focuses on how individual assessors or experts conduct risk evaluation [16,78,131], our data unveiled a distinctive approach where individuals collectively assessed privacy risks and engaged in speculative discussions. This collaborative process was driven by the complex and obscure nature of the post-Roe privacy landscape.

5.2.1 Risks of data subpoena and prosecution

In discussions about period and fertility tracking after the overturn of Roe, people made inferences based on their past knowledge or experience, speculating that they are at risk of data subpoena or prosecution. Specifically, many were worried that companies would directly comply with the request from authorities at the expense of user privacy. For example, a user wrote,

> U14: (…) Every single data point on you held by an American company, or a company in a country that could be held to US laws (treaties, locations in the US?), and can be used against you. This has BEEN a problem since pre-RIP roe, it just now specifically affects period tracking. No company will help you. You are not worth it to them.

This user highlighted that people's personal data are not safe with period and fertility tracking app companies because they might prioritize compliance with authorities over user privacy, exposing them to the risk of prosecution. They argued that companies had already complied with legal authorities' requests before the overturn of Roe v. Wade, which is not mere speculation but backed by prior investigation [119]. They believed that the same thing would happen for period and fertility tracking apps post-Roe.

People also pointed out that even if a company is secure now, there is no guarantee for future security. For example, after a thread poster recommended two new "safer" apps, a user commented,

> U15: Until they get bought. Until they have a powerful right-winger on the board. Until they get subpoenaed. NO APP IS SAFE.

In response to the safer app recommendation, U15 questioned the claims and speculated the potential risks associated with the companies behind the apps, suggesting that changes in political affiliations, personnel, ownership stakes, or receiving data requests from the government may impact their commitment to privacy protection. Therefore, U15 advocated caution, suggesting unforeseen risks could arise with time.

Beyond worries about data subpoenas, there is speculation on how authorities might use period and fertility tracking data in litigation. Litigation risk refers to the risk that an individual or corporation will face legal action [95]. In a discussion,

> U16: Can your period apps actually be used against you in a court of law? (…) Period tracker apps rely on us to manually input our cycle into them. How would it be possible

> to prove that someone was not menstruating when they were supposed to and that they didn't just forget to log it for that period of time? (...)
>
> U17: You don't "prove" things in a court of law, you convince people with arguments. The logs of your period app would be one piece of evidence that the other side would use as part of their argument (...) They wouldn't "just" use your app, they would use it "in conjunction with other things," like the fact that you don't have a history of forgetting to input the data (...) or your browser history shows you visiting Planned Parenthood sites around that same time, etc. (...) if they have access, it absolutely could be used against you. *Anything can. *

U16 highlighted the potential unreliability of self-reported data. This speculation stems from the difficulty of verifying the accuracy of this data in a legal context. U17 countered that in legal battles, the objective is persuasion over mere proof. They suggested that while period tracking data might not be sufficient evidence, when coupled with other indicators, it could build a compelling case. This implied the user's speculation on how aggregating personal data from various sources might increase potential legal risks for individuals.

5.2.2 Risks of state surveillance and monitor

When speculating about the risks of period and fertility tracking post-Roe, many expressed their concerns about state surveillance. State surveillance involves the monitoring, collecting and analysing of personal information by the government or state authorities. People feared that authorities would monitor citizens and identify those who have had abortions using period and fertility tracking data. In a discussion,

> U18: What's ridiculous is people think "the state" is going to be tracking them.
> U19: There is precedent for state governments to monitor detailed personal information to identify abortionists. The director of the Missouri state health department admitted that the state monitored detailed personal information about Planned Parenthood patients, in some cases reviewing women's menstrual cycles, intending to identify those who had had "failed medical abortions."

U18 dismissed the notion that "the state" would track individuals, implying that it is an unrealistic belief. U19 countered this by referencing a precedent where a state government monitored personal details to identify individuals who had abortions [140]. U19 implied that this specific incident is not an isolated case and suggested the risks of state surveillance in similar contexts.

Many also speculated that even if they try to hide their health information, authorities could still easily access and piece together such information with technological methods. In a post about state surveillance,

> U21: Even if you use fake accounts to use period tracking app, fake accounts can still be linked to your device (...) so your data can still be combined. It also gets more sinister when datasets can be linked by device or some other ID, data collected by one company can be combined with completely unrelated information from another. It's wild out there.

The user believed that there could be multiple methods for authorities to link a person with their personal information, undermining their privacy precautions. People felt that common practices they use to protect their data privacy were not effective. In this case, people speculated that they were subject to state surveillance and powerless to protect themselves.

5.2.3 Risks of privacy invasion and harassment

People also expressed their concerns about privacy invasion and harassment from other people such as anti-abortion groups. Their speculation has a cultural and social context. Specifically, the abortion debate has been ongoing in the United States for decades [32]. Many people oppose abortion on moral and religious grounds and support a legal ban or restriction on abortion, and have organized movements to promote the idea [137]. For example, some organized harassment and even anti-abortion violence on people who sought or appeared to be seeking abortions [69,94]. In our dataset, many expressed concerns about the privacy risks associated with period and fertility tracking apps, fearing that breaches could lead to harassment. For example,

> U22: We aren't free. A single accident, a single sexual assault, or a single contraceptive failure will reduce us to breeding mares. There's even talk of using period trackers to harass those who miss their period.

This user reacted strongly to the Roe v. Wade overturn, using phrases such as "aren't free" and "breeding mares" to stress how much could be at stake if an unwanted pregnancy happens. They also shared that they observed existing threats of using period trackers to harass people who miss their periods.

People also speculated about whether and how anti-abortion groups could access people's period tracking data for harassment purposes. For example,

> U23: (...) A big issue is that US pro-life groups could just buy these data, and harass people who got pregnant and stopped being pregnant, including those who had a miscarriage.

This user expressed their concern that their menstrual cycle data could be available on the market and that pro-life groups might easily buy the data to identify and harass people, no matter whether it is abortion or miscarriage. While the actual likelihood of such events would depend on various factors such as practices of these apps and behaviors of other stakeholders, there have been past instances where sensitive personal data has been sold or misused, making the user's concerns not entirely unfounded [55].

People also speculated that with the rise of big data, companies, and anti-abortion people could compound to pose greater privacy risks. For example,

> U24: The web of big data can be used to figure out way too much about your personal life. This older article (URL redacted) talks about how companies can know a person is pregnant because of subtle changes in seemingly unrelated habits. An individual data point is meaningless, but big data like this could be used to make suspect lists of people to harass and intimidate.

The user speculated that companies collected vast amounts of user data, from which companies could analyze the behavioral patterns of users such as shopping habits, personal habits, and, in this case, menstrual cycle patterns, which is not baseless [49]. People were concerned that data analytics might pinpoint individuals who are likely to have an abortion or miscarriage, making them potential targets for harassment.

5.2.4 Emotional ramifications and mental health risks

People inferred from their past experiences and their understanding of current privacy issues in period and fertility tracking, pointed out the possible emotional ramifications and mental health risks they might experience. For example,

> U25: I like the electronic ones because they automatically calculate my average cycle length (…) I think if they made the ban federal I'd be way too scared to use the apps anymore, even with someone else's assistance. Their benefits are not worth the potential costs at the end of the day.

The user tentatively preferred period and fertility tracking apps but emphasized they may reconsider based on changing laws. They emphasized that they might experience fear if stricter anti-abortion laws emerge, and that the privacy risks of using these apps in this context might be too emotionally taxing for them.

Many also noted the risks from being mistakenly flagged for abortion because of tracking data anomalies. For example,

> U20: Even if you had a spontaneous/natural miscarriage, you could still be considered as a "suspect." Can you imagine the pain of losing a very wanted baby and then being scrutinized and villainized by the government?

This user speculated the risk of being prosecuted even when having a natural miscarriage, articulating the risk by describing a heart-breaking scenario. This user highlighted that misplaced suspicion or prosecution based on anomalies in period and fertility tracking data could cause legal hassles and great mental harm to people who have experienced miscarriages and are already suffering.

5.3 Resisting Data Surveillance

Perceiving emergent privacy risks following the overturn, Reddit users also brainstormed means of resisting potential data surveillance. In contrast to previous research, which centered on individual-level mitigation [42,61], the data in this study revealed that Reddit users not only focused on individual-level measures but also on addressing privacy risks collectively. They engaged in collective actions to safeguard their shared interests and protect their privacy as a community.

Data surveillance refers to the monitoring of personal information and period and fertility tracking data by entities, such as government agencies and companies. To address this issue, they came up with various approaches to track their menstrual cycle in a safer way. Specifically, people shared their intention to abandon the use of period and fertility tracking apps. For example,

> U26: If (…) your period comes 6 weeks late, that could be interpreted any type of way by politicians and law enforcement. Granted, this is all based on historical data being present and your historical data being relatively predictable. Not using the apps is just the best security practice, but as with anything, your level of acceptable risk may vary.

The user first pointed out legal institutions' great jurisdiction in the prosecution of abortion. Then they argued that the prosecution is based on users' historical data, such as the data they entered into period and fertility tracking apps. The user emphasized that stopping using tracking apps could certainly reduce such risk and suggested that those who want more security abandon them.

Together, people also envisioned how they could continue to conveniently track period and fertility data while protecting their privacy. In a discussion,

> U27: A European-based app would be the work-around? (…) EU countries will tell the US to piss off, because it would be a violation of individual privacy.

> U28: I'm a software developer (…) I will donate my time to write this in C++, C#, python, cobalt, perl, or whatever language.
> U29: You'd really want to use a master-key style situation to encrypt the data. (…) This way the user can oversee their own privacy and protect data from being decrypted from a MITM attack.
> U30: I am a student, and I can help you however I can.

After U27 suggested choosing a European-based app to mitigate post-Roe risks, all three users further responded by offering the support of creating an alternative, safer tracking app for more people. This case showed how people were willing to collaborate and provide various forms of social support, such as U27's informational support, U28 and U30's intellectual and instrumental support to develop a new app, and U29's informational feedback to refine the new app's ideation.

Brainstorming ways to resist data surveillance was a dynamic, iterative, and constant practice that people needed to engage in because new privacy risks were always emerging. For example, in a discussion,

> U31: In the old days you just marked your periods on a calendar. Worked just fine.
> U32: Just name it something with a random word or phrase like "water the plants" …
> U33: I use the big red dot emoji
> U34: You've never heard of pattern recognition

Users 31, 32, and 33 here discussed different ways of mitigating the privacy risks of tracking menstruation manually on calendars. However, U34 pointed out a persistent risk that certain authorities can still use pattern recognition, a data analysis technique, to identify anomalies in manually tracked data, identifying potential abortions. The above thread thus showed that even if a way of resisting surveillance was considered secure enough by many, people were still constantly thinking and uncovering new risks that might arise in the process.

Many Reddit users, regardless of gender or identity, envisioned collective activism against surveillance to resist surveillance. For example,

> U35: Those of us who are male and supportive of reproductive rights can muddy the waters of digital surveillance by filling out bogus data in period tracking apps, bogus texts, Google searches, etc. (…) the data will be hopelessly full of garbage.

U35 expressed a belief in the power of collective actions to combat surveillance proactively, suggesting multiple ways of spreading inaccurate and deceptive health data. The purpose of this proposed action was to undermine the reliability and validity of potential sources of evidence that authorities might rely on, such as period tracking apps or online search data. The goal was to reduce the data's reliability in legal cases related to reproductive health, thereby resisting surveillance and safeguarding privacy.

Many also advocated for political engagement to establish legal safeguards against surveillance of reproductive health data from the ground up. For example,

> U36: The algorithm will be messy, but someone can still have their personal data subpoenaed and used against them in court. So, the best thing you can do is hold your male peers accountable and pack your ballot with Democrats so we can end the filibuster and codify Roe.

U36 noted that even if people messed up the data in period and fertility tracking apps, authorities still could subpoena it. Therefore, in order to fundamentally protect people's

reproductive and privacy rights, the user essentially encouraged individuals to vote for Democratic candidates who were more likely to support reproductive rights and work towards legislative action on the issue. By this, the user hoped to promote certain policy goals, such as ending the filibuster to facilitate the passage of legislation related to reproductive rights, and resist state surveillance.

6 DISCUSSION

Through an analysis of post-Roe collective privacy sensemaking on social media, we examined how people collectively contextualize the privacy of period and fertility tracking, speculate about related risks and propose collaborative actions to protect their privacy. Next, we discuss this set of findings, which provide insights into the evolving landscape of privacy concerns. Individuals are actively engaging in collective sensemaking on online platforms to make sense of the complex privacy and legal concerns that have emerged in period and fertility tracking practices. It sheds light on the multifaceted challenges individuals face when navigating reproductive healthcare decisions, which suggests that the privacy issues observed are part of a broader discourse on the intersection of healthcare, privacy, and personal autonomy.

6.1 Collective Privacy Sensemaking: Characteristics, Benefits, and Limits

Previous research focused primarily on individual and group privacy sensemaking and decision-making. Concepts such as privacy calculus and privacy paradox tend to emphasize individual-level decision making [18,45,99]. For instance, privacy calculus theory assumes that individuals evaluate expected benefits and perceived risks in order to make rational decisions about the disclosure of their personal data [45]. Privacy paradox denotes the mismatch between individuals' privacy attitudes and actions [18]. In addition, studies of collective privacy management in groups focus on how individuals engage in collaborative strategies when sharing information related to multiple individuals in their groups [26,89]. Collective privacy sensemaking moves beyond the scales of the individual and the group, to concern how a collective responds to privacy risks and advocates privacy actions at the scales of community or society. In our study, Reddit facilitated the formation of such a collective to actively engage in discussion, sharing information and personal experiences, evaluating the privacy risks associated with specific apps, speculating about potential risks, and envisioning individual and collective privacy actions.

The post-Roe, privacy landscape engenders a pressing need for collective privacy sensemaking to cope with a challenging privacy situation, especially given the added legal complexities. We found that people must gather and analyze vast and intricate information to comprehend both the privacy and legal risks associated with period and fertility tracking. The complexities and uncertainties within this landscape could pose challenges for individual-level decision-making [1,155]. However, collective sensemaking offers distinct advantages for individuals to cope with the privacy challenges by facilitating collaborative information sharing, idea exchange, and narrative building [40,166]. Collective sensemaking brings the richness of perspectives and fosters collaboration, which could help uncover hidden or overlooked dimensions of privacy risks that individual sensemaking may miss [120,147]. Consequently, it can reduce the risk of cognitive biases and blind spots that may hinder an individual's privacy assessment. Our findings have many examples of Reddit users countering the views of other users and providing evidence to support their counterpoints. They collectively gathered information, developed narratives and proposed potential solutions, which raised awareness about privacy threats in period and fertility tracking.

In addition, collective privacy sensemaking fosters a sense of collective agency and serves as a catalyst for privacy activism. Previous research has shown that personal experience sharing, community building, and the development of shared narratives facilitate online activism [2,68]. Our study further provided empirical evidence for the connection between collective sensemaking and privacy activism. We observed that when individuals engage in collective sensemaking by sharing their concerns and collectively identifying and assessing privacy-related risks, it motivates them to take action and practice privacy activism. Additionally, the concept of collective resilience comes into play, representing the ability of people to achieve positive outcomes despite challenging circumstances [47,50]. In the context of our study, people engaging in collective sensemaking and practicing privacy activism demonstrates collective resilience to strive for positive changes in privacy practices and policies, even in the face of obstacles or resistance. Echoing previous studies, the privacy activism strategy people envision often aims to challenge the power dynamic in current data practices and fight surveillance [71,112]. For instance, some suggested inputting inaccurate and deceptive health data in period tracking apps, believing it could compromise the data's reliability and its use for harvesting or legal purposes. However, experts have pointed out that such tactics merely add noise, which robust algorithms can filter out [75]. Additionally, too much erroneous data intends to confuse the algorithms, making the apps less accurate or even useless for the intended users [75]. The fact that the experts' views conflict with the speculations and visions of these users is a reflection of how users' understanding of data technologies affects their sensemaking of privacy. Due to the black box and non-transparent nature of big data, it is difficult for people to identify the optimal solution to protect their privacy.

Despite the advantages, collective privacy sensemaking of these apps can also amplify speculation and distrust due to the lack of transparency in their privacy practices. Previous studies have revealed that people may collectively develop narratives, make speculation and even come up with conspiracy theories to cope with uncertainties and the lack of transparent information [13,100]. Our study provided empirical evidence demonstrating how people collectively make inferences and speculation to cope with uncertainties in privacy sensemaking. For example, our study revealed that due to the lack of transparency of the data practices of period and fertility tracking apps, individuals expressed concerns, shared worries and collaboratively speculated about potential privacy and legal risks, intensifying a collective sense of unease and distrust.

In addition, collective privacy sensemaking is not immune to inherent cognitive biases. Social biases, such as the bandwagon effect, pointed out potential biases that individuals adopt beliefs because they perceive them to be popular within a group, or shared information bias, where group discussions tend to focus on information all members already know [141]. The complex and opaque privacy landscape post-Roe could cause individuals to believe explanations and narratives that they encounter repeatedly and deem credible. For instance, we observed that uncertainties, fear and a strong desire to protect personal privacy, combined with exposure to limited and focused information, prompted many to believe that inputting false data into period tracking apps can mislead the algorithm and hide their data, even though little evidence supports this belief. Thus, it is essential to approach collective privacy sensemaking with critical discernment to identify misleading narratives and differentiate between validated information and popular opinion while recognizing the inherent advantages of such discussions.

Implications for Design:

Our study revealed the benefits of collective privacy assessment and privacy actions facilitated by social media. Thus, we suggest that social media platforms should foster a collaborative environment where users can engage in privacy sensemaking collectively. Social media platforms can also incorporate features that support data activism efforts such as facilitating data-driven storytelling. Our findings revealed that people's understanding of data technologies greatly impacts their privacy assessment. Thus, we suggest that privacy design should prioritize transparency in communicating how data technologies operate and how user data is collected, processed, and shared.

6.2 Privacy Concern and Legal Implication in the post-Roe Context

Before the overturn of Roe, HCI research has extensively studied the privacy of period and fertility tracking apps, highlighting the shortcomings in their data practices [4,53,60,110,143]. In addition, prior studies also underscored the lack of federal privacy laws and inadequate data regulation regarding these apps [98,104,135], and discussed the legal practices of using digital traces such as search history in courts [15,24,33,41,114]. After the overturn of Roe v. Wade, the privacy of period and fertility tracking became more pronounced. Many states have started banning abortion, and there are emerging warnings about the potential use of period tracking data in courts [34,63], leading to increased concerns about user privacy [63]. In light of these evolving circumstances, our research foregrounds the end users' perspectives, revealing how users' understanding of the ownership of their health data and legality impacted their privacy sensemaking.

What is in question here is data ownership, or who owns the data. Data ownership can be a defensive, protective concept regarding personal privacy [62,83]. Data ownership, as a concept, is also complex and varies depending on legal systems and jurisdictions [77]. Outside the U.S., the GDPR does not explicitly address the concept of data ownership [85]. However, it indirectly recognizes the importance of data ownership through the rights it grants to individuals, such as providing individuals with control and decision-making power over their personal data [85]. In contrast, in the U.S., the existing policies and laws are inadequate in recognizing the importance of data ownership regarding period and fertility tracking apps. There is a lack of uniform, comprehensive and well-developed federal data privacy laws that address the privacy protection of health data. Furthermore, there is a significant absence of privacy laws and regulations specifically tailored to address the unique context of period and fertility tracking apps [98,104,135]. While HIPAA offers some protection for individuals' medical information, it does not extend coverage to the self-reported period and fertility tracking data stored within these apps. Compounding the issue, there have been instances where period and fertility tracking apps have shared user data with third parties [70,134]. As such, the lack of data ownership when it comes to one's reproductive data, and its legal consequences, cause serious distress and concerns. Our findings suggested that many people have experienced their own data being shared with third parties by period and fertility tracking apps without their consent, an experience that has heightened their concerns about losing personal privacy.

A lack of data ownership means that reproductive data stored in period and fertility tracking apps could be accessible to multiple parties [39,48,117,142]. Our study revealed users' speculations about potential data access routes: (1) law enforcement accessing data via legal methods, such as subpoenas, (2) anti-abortion people buying data from brokers, and (3) data analytics creating lists potentially used for harassment by anti-abortion people. Thus, people highlighted that when multiple groups are present, they both bring distinct risks and compound other groups' risks.

Such risk compounding only serves to exacerbate the already grave privacy concerns about period and fertility tracking apps.

When the legal protection of data ownership is lacking, the legality of such period tracking data becomes a logical next concern, especially in light of prior legal practices of using digital traces in courts [15,24,41,114]. Digital forensics has increasingly become pivotal in criminal investigations [15,41]. While this practice is often viewed with suspicion due to concerns of authenticity and uncertainty, there are instances where its use is deemed justified [15,24,138]. In the U.S., police and prosecutors have extracted evidence for a wide range of crimes, including graffiti, shoplifting, and prostitution [33]. There is precedent for women's reproductive health-related search records being used as evidence of criminal intent [33,103]. Thus, it is reasonable that legal scholars worry that the inclusion of digital evidence such as internet search history will become standard protocol nationwide after the recriminalization of abortion [33]. However, our analysis of the end users' perspective provided several new insights into this legality issue. If digital traces are expected to be an accurate reflection of facts, then period and fertility tracking data does not satisfy this basic expectation. In our findings, many mentioned the unreliability of self-reported data in period tracking apps. For instance, a missed period log could result from user oversight rather than an abortion. Besides, spontaneous abortion can cause abnormalities in the menstrual cycle similar to those associated with abortion. These reasonings have scientific basis [30,123,127], but may not prevent suspicious eyes from authorities and even further legal investigations.

What further challenges the legality of period and fertility tracking data is data activism [71,112], in which people reject the role of being passively observed, but actively engage with the data system, seeking to "alter the power distribution" [71,112]. Previous research has highlighted collective actions for user empowerment and improved privacy [139,170]. Our study further revealed how people challenge the current power dynamics in both data and legal practices. For example, they envisioned strategies like inputting garbage data into tracking apps to compromise data credibility for litigation and impede efforts to identify abortion cases via data analysis. People addressed massive data collection as both a challenge to privacy rights and a novel set of opportunities for privacy actions and social change.

Implications for Policymaking:

Although period and fertility tracking data is a kind of sensitive health data, it is not protected by HIPAA [122]. With the rapid development of mobile health applications, we suggest there should be privacy laws that cover the protection of period and fertility tracking data and other kinds of self-report data stored in mobile health apps. In addition, there should be a clear delineation of data ownership, thus regulating the responsibility of each party for data protection. The legality of period and fertility tracking data used in criminal investigation also requires further discussion. Policymakers need to understand the unique nature of this health data, and that anomalies in this data may have multiple explanations.

6.3 State Surveillance and Bodily Autonomy

Before the overturn of Roe v. Wade, the state surveillance of people's personal data had already drawn great attention [12,105]. With the overturn of Roe v. Wade and many states banning abortion [32,97], state surveillance implies that legal authorities may find evidence of a user's possible abortion from large amounts of user data. Our study vividly demonstrated users' concerns about being monitored and losing their bodily autonomy in the new context.

Traditional understandings of the operations of surveillance and its social consequences are being reconstructed by big data [12,105]. The large amount of easily accessible data, including online searches, location tracking, and health tracking data, broadens the power of state surveillance, and enables authorities to monitor people and identify those who might have had abortions [33]. Our study found that users recognized instances where authorities monitored sensitive information, such as Planned Parenthood visits, to pinpoint potential abortions. Given this enhanced surveillance and the post-Roe abortion bans, many chose to avoid period and fertility apps, fearing it could compromise their reproductive health autonomy.

Bodily autonomy is the right of an individual to exercise autonomy (any choice or decision) over their body and is a fundamental human right [76,92]. Our study echoes previous studies, highlighting the role of period and fertility tracking apps in managing reproductive health, like monitoring cycles and detecting irregularities, thereby giving individuals better bodily control [36,37,162]. Yet, aligning with a previous study [108], we noted that many period and fertility tracking app users were abandoning or considering abandoning their familiar ways of tracking this data due to heightened privacy and legal concerns. Such apprehensions deter app utilization, risking a loss of crucial health insights, which could compromise reproductive health management. This fear of being monitored may disproportionately affect marginalized communities, including those with special reproductive health care needs or illnesses.

Menstrual self-tracking is closely related to self-identity and serves as a means of self-liberation and personal empowerment in the deep-rooted menstrual stigma context [80,162]. However, the overturn of Roe v. Wade led many to abandon familiar methods of period tracking, deeply affecting their sense of self and mental well-being. For example, our findings revealed that this loss of bodily autonomy induced significant anxiety, stress, and mental health challenges. A user vividly described themselves as "not free" and feeling like "breeding mares," illustrating the overwhelming sense of powerlessness. Such sentiments reflect the erosion of personal agency and the inability to safeguard their well-being. We observed a wide range of negative emotions such as frustration, sadness and anger when people collectively made sense of the significant privacy risks in period and fertility tracking apps post-Roe. The convergence of menstrual stigma, the restriction of bodily autonomy, and the heightened privacy risks has resulted in a multifaceted and distressing environment for women and people with uteruses. This combination of factors intensifies their apprehension within an already challenging landscape.

While our findings are situated in the privacy landscape of the U.S., it is imperative to understand that privacy concerns about reproductive health extend well beyond the U.S. context. Though our findings primarily address the U.S. context, they are notably shaped by global privacy frameworks such as GDPR—particularly when some period and fertility tracking apps or their partnering entities operate within the EU. This emphasizes the interconnectedness of privacy concerns on a global scale, suggesting they are not isolated to any one locale. Moving beyond the U.S., it becomes clear that the nuances in privacy risks are more than just regional variations. They are deeply intertwined with the cultural, political, and legal fabric of each region. This connection is particularly pronounced in regions where women and those with reproductive capabilities face amplified oppression, up against systemic marginalization, societal biases, and potentially harsh legal consequences [7,64]. Yet, amidst these challenges lies a silver lining: the potential for transformative policy. While frameworks like GDPR offer a relatively comprehensive approach, they emerge from a predominantly Western context [133,168]. The nuances of each region's challenges urge us toward the creation of adaptive regulations, sensitive to local exigencies. Moreover, our findings underscore the call to action for individuals,

communities, and global entities to proactively design measures that empower reproductive autonomy, especially when navigating oppressive state mechanisms.

Implications for Policymaking:

We suggest that policymakers need to fully consider the importance of period and fertility tracking for people to take control of their bodies and monitor their health. Authorities should respect citizens' right to privacy and protect their right to health. Inappropriate monitoring of people's health data can force them to abandon their familiar tools for healthcare and pose health risks and mental hazards to people. Policymakers need to respect people's right to make choices about their own body without coercion or violence.

7 CONCLUSIONS

We reported an analysis of collective sensemaking in the post-Roe time, investigating how individuals collaboratively assess privacy with contextual information, speculate about associated risks, and brainstorm strategies to protect their privacy. Given the intricate and contextual nature of privacy, collective sensemaking offers distinct advantages in navigating the complex landscape of privacy concerns post Roe. It allows individuals to collectively assess the potential risks and brainstorm means to fight surveillance, although their sensemaking is still affected and limited by data literacy, technology understanding, and the apps' opaque data practices. However, collective sensemaking could also amplify speculation and distrust due to ambiguities. People question the legality of period and fertility tracking data but also express grave concerns about the legal implications of it. Such legal risk compounds people's existing privacy concerns about their period and fertility tracking data, putting them in a further vulnerable position and perpetuating the oppression over the individual's body.

ACKNOWLEDGMENTS

We appreciate the thoughtful and detailed feedback from the ACs and external reviewers. This work was partially supported by the Penn State College of Information Sciences and Technology's seed grant program.

REFERENCES

[1] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. IEEE security & privacy 3, 1 (2005), 26–33.

[2] Manju Ahuja, Pankaj Patel, and Ayoung Suh. 2018. The influence of social media on collective action in the context of digital activism: An affordance approach. In Proceedings of the 51th Hawaii International Conference on System Sciences, 2018. 2203–2212. https://doi.org/10.24251/HICSS.2018.275

[3] Shaden Al-Aqeeli, Mznah Al-Rodhaan, and Yuan Tian. 2017. Privacy preserving risk mitigation strategy for access control in e-healthcare systems. In 2017 International Conference on Informatics, Health & Technology (ICIHT), 2017. 1–6. https://doi.org/10.1109/ICIHT.2017.7899150

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

[5] Roshonara Ali, Zeynep B. Gürtin, and Joyce C. Harper. 2021. Do fertility tracking applications offer women useful information about their fertile window? Reproductive BioMedicine Online 42, 1 (January 2021), 273–281. https://doi.org/10.1016/j.rbmo.2020.09.005

[6] Teresa Almeida, Madeline Balaam, and Rob Comber. 2020. Woman-Centered Design through Humanity, Activism, and Inclusion. ACM Trans. Comput.-Hum. Interact. 27, 4 (September 2020). https://doi.org/10.1145/3397176

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

(NordiCHI '22), 2022, New York, NY, USA. Association for Computing Machinery, New York, NY, USA. . https://doi.org/10.1145/3547522.3547674

[8] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15), 2015, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 787–796. https://doi.org/10.1145/2702123.2702210

[9] Nazanin Andalibi and Andrea Forte. 2018. Announcing Pregnancy Loss on Facebook: A Decision-Making Framework for Stigmatized Disclosures on Identified Social Network Sites. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18), 2018, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3173732

[10] Nazanin Andalibi, Oliver L. Haimson, Munmun De Choudhury, and Andrea Forte. 2016. Understanding Social Media Disclosures of Sexual Abuse Through the Lenses of Support Seeking and Anonymity. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16), 2016, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 3906–3918. . https://doi.org/10.1145/2858036.2858096

[11] Nazanin Andalibi, Pinar Ozturk, and Andrea Forte. 2017. Sensitive Self-Disclosures, Responses, and Social Support on Instagram: The Case of #Depression. In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17), 2017, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 1485–1500. https://doi.org/10.1145/2998181.2998243

[12] Mark Andrejevic and Kelly Gates. 2014. Big data surveillance: Introduction. Surveillance & Society 12, 2 (2014), 185–196. https://doi.org/10.24908/ss.v12i2.5242

[13] Cynthia Andrews, Elodie Fichet, Yuwei Ding, Emma S. Spiro, and Kate Starbird. 2016. Keeping Up with the Tweet-dashians. In Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16), 2016. ACM, 452–465. https://doi.org/10.1145/2818048.2819986

[14] Shaden Aqeeli, Mznah Al-Rodhaan, Yuan Tian, and Abdullah Al-Dhelaan. 2018. Privacy Preserving Risk Mitigation Approach for Healthcare Domain. E-Health Telecommunication Systems and Networks 07, (January 2018), 1–42. https://doi.org/10.4236/etsn.2018.71001

[15] Arshad Humaira, Jantan Aman Bin, and Abiodun Oludare Isaac. 2018. Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. Journal of Information Processing Systems 14, 2 (April 2018), 346–376. https://doi.org/10.3745/JIPS.03.0095

[16] Terje Aven. 2016. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research 253, 1 (2016), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

[17] James A. Banks. 1998. The Lives and Values of Researchers: Implications for Educating Citizens in a Multicultural Society. Educational Researcher 27, 7 (1998), 4–17. https://doi.org/10.2307/1176055

[18] Susan B Barnes. 2006. A privacy paradox: Social networking in the United States. First Monday 11, (2006). https://doi.org/10.5210/fm.v11i9.1394

[19] M Antonia Biggs and Corinne Rocca. 2022. Forecasting the mental health harms of overturning Roe v Wade. BMJ 378, (July 2022), o1890. https://doi.org/10.1136/bmj.o1890

[20] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. Qualitative research in psychology 3, 2 (2006), 77–101.

[21] Andrew D. Brown, Ian Colville, and Annie Pye. 2015. Making Sense of Sensemaking in Organization Studies. Organization Studies 36, 2 (2015), 265–277. https://doi.org/10.1177/0170840614559259

[22] Elizabeth A. Brown. 2021. THE FEMTECH PARADOX: HOW WORKPLACE MONITORING THREATENS WOMEN'S EQUITY. Jurimetrics 61, 3 (2021), 289–329.

[23] Nadia Campo Woytuk, Linette Nilsson, and Mingxing Liu. 2019. Your Period Rules: Design Implications for Period-Positive Technologies. In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19), 2019, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3290607.3312888

[24] Eoghan Casey. 2002. Error, uncertainty, and loss in digital evidence. International journal of digital evidence 1, 2 (2002), 1–45.

[25] Centers for Disease Control and Prevention. 2022. Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC. Retrieved April 15, 2023 from https://www.cdc.gov/phlp/publications/topic/hipaa.html

[26] Hichang Cho and Anna Filippova. 2016. Networked Privacy Management in Facebook: A Mixed-Methods and Multinational Study. In Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16), 2016, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 503–514. https://doi.org/10.1145/2818048.2819996

[27] Hichang Cho, Bart Knijnenburg, Alfred Kobsa, and Yao Li. 2018. Collective Privacy Management in Social Media: A Cross-Cultural Validation. ACM Trans. Comput.-Hum. Interact. 25, 3 (June 2018). https://doi.org/10.1145/3193120

[28] Clue. 2023. Period tracking can be a revelation. Retrieved June 27, 2023 from https://helloclue.com/

[29] Karine Coen-Sanchez, Bassey Ebenso, Ieman Mona El-Mowafi, Maria Berghs, Dina Idriss-Wheeler, and Sanni Yaya. 2022. Repercussions of overturning Roe v. Wade for women across systems and beyond borders. Reproductive Health 19, 1 (August 2022), 184. https://doi.org/10.1186/s12978-022-01490-y

[30] Judy Slome Cohain, Rina E Buxbaum, and David Mankuta. 2017. Spontaneous first trimester miscarriage rates per woman among parous women with 1 or more pregnancies of 24 weeks or more. BMC pregnancy and childbirth 17, 1 (2017), 1–7.
[31] I. Glenn Cohen, Judith Daar, and Eli Y. Adashi. 2022. What Overturning Roe v Wade May Mean for Assisted Reproductive Technologies in the US. JAMA 328, 1 (July 2022), 15–16. https://doi.org/10.1001/jama.2022.10163
[32] Sarah Compton and Scott L. Greer. 2022. What overturning Roe v. Wade means for the United States. BMJ 377, (May 2022), o1255. https://doi.org/10.1136/bmj.o1255
[33] Cynthia Conti-Cook. 2020. Surveilling the Digital Abortion Diary. U. Balt. L. Rev. 50, (2020), 1.
[34] Bethany Corbin. 2022. Femtech Data Privacy and the Changing Abortion Landscape: What Femtech Companies and Founders Need to Know. Nixon Gwilt Law. Retrieved October 7, 2022 from https://nixongwiltlaw.com/nlg-blog/2022/5/16/femtech-data-privacy-and-the-chaning-abortion-landscape-what-femtech-companies-and-founders-need-to-know
[35] Juliet Corbin and Anselm Strauss. 2014. Basics of qualitative research: Techniques and procedures for developing grounded theory. Sage publications.
[36] Mayara Costa Figueiredo, Clara Caldeira, Elizabeth Victoria Eikey, Melissa Mazmanian, and Yunan Chen. 2018. Engaging with Health Data: The Interplay Between Self-Tracking Activities and Emotions in Fertility Struggles. Proc. ACM Hum.-Comput. Interact. 2, CSCW (November 2018). https://doi.org/10.1145/3274309
[37] Mayara Costa Figueiredo, H. Irene Su, and Yunan Chen. 2021. Using Data to Approach the Unknown: Patients' and Healthcare Providers? Data Practices in Fertility Challenges. Proc. ACM Hum.-Comput. Interact. 4, CSCW3 (January 2021). https://doi.org/10.1145/3432926
[38] David Cox. 2022. How overturning Roe v Wade has eroded privacy of personal data. BMJ 378, (August 2022), o2075. https://doi.org/10.1136/bmj.o2075
[39] Joseph Cox. 2022. Data Broker Is Selling Location Data of People Who Visit Abortion Clinics. Vice. Retrieved January 14, 2023 from https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood
[40] Graeme Currie and Andrew D Brown. 2003. A narratological approach to understanding processes of organizing in a UK hospital. Human Relations 56, 5 (2003), 563–586.
[41] Bart Custers and Lonneke Stevens. 2021. The Use of Data as Evidence in Dutch Criminal Courts. European Journal of Crime, Criminal Law and Criminal Justice 29, 1 (April 2021), 25–46. https://doi.org/10.1163/15718174-bja10015
[42] Francis J. D'Addario. 2013. Chapter 4 - Prioritizing Risk Mitigation. In Influencing Global Risk Mitigation, Francis J. D'Addario (ed.). Elsevier, Boston, 47–58. https://doi.org/10.1016/B978-0-12-417233-3.00004-8
[43] Dharma Dailey and Kate Starbird. 2015. "It's Raining Dispersants": Collective Sensemaking of Complex Information in Crisis Contexts. In Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing (CSCW'15 Companion), 2015, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 155–158. https://doi.org/10.1145/2685553.2698995
[44] Sourya Joyee De and Daniel Le Métayer. 2016. PRIAM: a privacy risk analysis methodology. In Data privacy management and security assurance. Springer, 221–229.
[45] Tamara Dinev and Paul Hart. 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research 17, 1 (March 2006), 61–80. https://doi.org/10.1287/isre.1060.0080
[46] Zikan Dong, Liu Wang, Hao Xie, Guoai Xu, and Haoyu Wang. 2023. Privacy Analysis of Period Tracking Mobile Apps in the Post-Roe v. Wade Era. In Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering (ASE '22), 2023, New York, NY, USA. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3551349.3561343
[47] John Drury, Chris Cocking, and Steve Reicher. 2009. The nature of collective resilience: Survivor reactions to the 2005 London bombings. International Journal of Mass Emergencies & Disasters 27, 1 (2009), 66–95.
[48] Duffy Jennifer Korn. 2022. Search histories, location data, text messages: How personal data could be used to enforce anti-abortion laws | CNN Business. CNN. Retrieved January 14, 2023 from https://www.cnn.com/2022/06/24/tech/abortion-laws-data-privacy/index.html
[49] Charles Duhigg. 2012. How Companies Learn Your Secrets. The New York Times. Retrieved October 27, 2023 from https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html
[50] Guy Elcheroth and John Drury. 2020. Collective resilience in times of crisis: Lessons from the literature for socially effective responses to the pandemic. British Journal of Social Psychology 59, 3 (2020), 703–713.
[51] Kim VL England. 1994. Getting personal: Reflexivity, positionality, and feminist research. The professional geographer 46, 1 (1994), 80–89.
[52] Daniel A. Epstein, Nicole B. Lee, Jennifer H. Kang, Elena Agapie, Jessica Schroeder, Laura R. Pina, James Fogarty, Julie A. Kientz, and Sean Munson. 2017. Examining Menstrual Tracking to Inform the Design of Personal Informatics Tools. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17), 2017, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 6876–6888. https://doi.org/10.1145/3025453.3025635
[53] 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. https://doi.org/10.1109/TTS.2022.3160928

[54] European Data Protection Supervisor. 2023. Health | European Data Protection Supervisor. Retrieved April 16, 2023 from https://edps.europa.eu/data-protection/our-work/subjects/health_en

[55] Federal Trade Commission. 2022. FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations. Federal Trade Commission. Retrieved October 25, 2023 from https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other

[56] Eve C. Feinberg, Jennifer F. Kawwass, and Marcelle I. Cedars. 2022. Roe v Wade and the Threat to Fertility Care. Obstetrics & Gynecology 140, 4 (2022), 557–559. https://doi.org/doi:10.1097/AOG.0000000000004928

[57] Flo. 2023. Flo - ovulation calendar, period tracker, and pregnancy app. Flo.health - #1 mobile product for women's health. Retrieved June 27, 2022 from https://flo.health/

[58] Luciano Floridi. 2017. Group Privacy: A Defence and an Interpretation. In Group Privacy. Springer International Publishing, 83–100. https://doi.org/10.1007/978-3-319-46608-8_5

[59] Eureka Foong, Darren Gergle, and Elizabeth M Gerber. 2017. Novice and expert sensemaking of crowdsourced design feedback. Proceedings of the ACM on Human-Computer Interaction 1, CSCW (2017), 1–18.

[60] Sarah Fox, Noura Howell, Richmond Wong, and Franchesca Spektor. 2019. Vivewell: Speculating Near-Future Menstrual Tracking through Current Data Practices. In Proceedings of the 2019 on Designing Interactive Systems Conference (DIS '19), 2019, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 541–552. https://doi.org/10.1145/3322276.3323695

[61] Xavier Franch, Ron S. Kenett, Angelo Susi, Nikolas Galanis, Ruediger Glott, and Fabio Mancinelli. 2015. Chapter 14 - Community Data for OSS Adoption Risk Management. In The Art and Science of Analyzing Software Data, Christian Bird, Tim Menzies and Thomas Zimmermann (eds.). Morgan Kaufmann, Boston, 377–409. https://doi.org/10.1016/B978-0-12-411519-4.00014-8

[62] Hannah K.; DeMuro Galvin Paul R. 2020. Developments in Privacy and Data Ownership in Mobile Health Technologies, 2016-2019. Yearb Med Inform 29, 01 (August 2020), 032–043. https://doi.org/10.1055/s-0040-1701987

[63] Flora Garamvolgyi. 2022. Why US women are deleting their period tracking apps. The Guardian. Retrieved October 27, 2022 from https://www.theguardian.com/world/2022/jun/28/why-us-woman-are-deleting-their-period-tracking-apps

[64] Claudia García-Moreno, Henrica AFM Jansen, Mary Ellsberg, Lori Heise, and Charlotte Watts. 2005. WHO multi-country study on women's health and domestic violence against women. World Health Organization.

[65] Josh Gerstein and Alexander Ward. 2022. Exclusive: Supreme Court has voted to overturn abortion rights, draft opinion shows. POLITICO. Retrieved November 1, 2022 from https://www.politico.com/news/2022/05/02/supreme-court-abortion-draft-opinion-00029473

[66] Olivia Goldhill. 2019. "FemTech" is not and should not be a thing. Quartz. Retrieved January 15, 2023 from https://qz.com/1586815/why-femtech-is-a-sexist-category/

[67] Sarah Graham. 2022. We're horrified by the rejection of Roe v Wade—but abortion is not a universal right in the UK. BMJ 378, (August 2022), o1945. https://doi.org/10.1136/bmj.o1945

[68] Hedy Greijdanus, Carlos A de Matos Fernandes, Felicity Turner-Zwinkels, Ali Honari, Carla A Roos, Hannes Rosenbusch, and Tom Postmes. 2020. The psychology of online activism and social movements: relations between online and offline collective action. Current Opinion in Psychology 35, (October 2020), 49–54. https://doi.org/10.1016/j.copsyc.2020.03.003

[69] David A Grimes, Jacqueline D Forrest, Alice L Kirkman, and Barbara Radford. 1991. An epidemic of antiabortion violence in the United States. American journal of obstetrics and gynecology 165, 5 (1991), 1263–1268.

[70] Alisha Haridasani Gupta and Natasha Singer. 2021. Your App Knows You Got Your Period. Guess Who It Told? The New York Times. Retrieved January 7, 2023 from https://www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html

[71] Miren Gutierrez. 2018. Data Activism and Social Change. Palgrave Pivot Cham. https://doi.org/10.1007/978-3-319-78319-2

[72] Oliver L. Haimson, Jed R. Brubaker, Lynn Dombrowski, and Gillian R. Hayes. 2015. Disclosure, Stress, and Support During Gender Transition on Facebook. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15), 2015, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 1176–1190. https://doi.org/10.1145/2675133.2675152

[73] Keith N Hampton, Lauren Sessions Goulet, Lee Rainie, and Kristen Purcell. 2011. Social networking sites and our lives. Pew Internet & American Life Project Washington, DC.

[74] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using Personal Examples to Improve Risk Communication for Security & Privacy Decisions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14), 2014, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 2647–2656. https://doi.org/10.1145/2556288.2556978

[75] Alexander L. Hayes, Katie Siek, and Zaidat Ibrahim. 2022. No, submitting junk data to period tracking apps won't protect reproductive privacy. The Conversation. Retrieved June 28, 2023 from http://theconversation.com/no-submitting-junk-data-to-period-tracking-apps-wont-protect-reproductive-privacy-186257

[76] Jonathan Herring and Jesse Wall. 2017. The nature and significance of the right to bodily integrity. The Cambridge Law Journal 76, 3 (2017), 566–588. https://doi.org/10.1017/S0008197317000605

[77] Jacqueline Hicks. 2023. The future of data ownership: An uncommon research agenda. The Sociological Review 71, 3 (May 2023), 544–560. https://doi.org/10.1177/00380261221088120

[78] Tammy C. Hoffmann and Chris Del Mar. 2017. Clinicians' Expectations of the Benefits and Harms of Treatments, Screening, and Tests: A Systematic Review. JAMA Internal Medicine 177, 3 (March 2017), 407–419. https://doi.org/10.1001/jamainternmed.2016.8254

[79] Bryndl Hohmann-Marriott. 2023. Periods as powerful data: User understandings of menstrual app data and information. New Media & Society 25, 11 (2023), 3028–3046. https://doi.org/10.1177/14614448211040245

[80] Sarah Homewood. 2018. Designing for the Changing Body: A Feminist Exploration of Self-Tracking Technologies. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18), 2018, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 1–4. https://doi.org/10.1145/3170427.3173031

[81] Sally Howard and Geetanjali Krishna. 2022. Roe v Wade: How its scrapping will affect women worldwide. BMJ 378, (August 2022), o1844. https://doi.org/10.1136/bmj.o1844

[82] Shawn Hubler. 2022. Thousands Protest End of Constitutional Right to Abortion. The New York Times. Retrieved October 27, 2022 from https://www.nytimes.com/live/2022/06/24/us/roe-wade-abortion-supreme-court

[83] Patrik Hummel, Matthias Braun, and Peter Dabrock. 2021. Own Data? Ethical Reflections on Data Ownership. Philosophy & Technology 34, 3 (September 2021), 545–572. https://doi.org/10.1007/s13347-020-00404-9

[84] Information Commissioner's Office. 2022. What is special category data? Retrieved April 16, 2023 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[85] Intersoft Consulting. 2023. General Data Protection Regulation (GDPR) – Official Legal Text. General Data Protection Regulation (GDPR). Retrieved June 27, 2023 from https://gdpr-info.eu/

[86] Lynn A. Isabella. 1990. Evolving Interpretations as a Change Unfolds: How Managers Construe Key Organizational Events. AMJ 33, 1 (March 1990), 7–41. https://doi.org/10.5465/256350

[87] Carlos Jensen and Colin Potts. 2004. Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '04), 2004, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 471–478. . https://doi.org/10.1145/985692.985752

[88] Haiyan Jia and Eric P.S. Baumer. 2022. Birds of a Feather: Collective Privacy of Online Social Activist Groups. Comput. Secur. 115, C (April 2022). https://doi.org/10.1016/j.cose.2022.102614

[89] Haiyan Jia and Heng Xu. 2016. Autonomous and Interdependent: Collaborative Privacy Management on Social Networking Sites. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16), 2016, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 4286–4297. . https://doi.org/10.1145/2858036.2858415

[90] Marc Jofre, Diana Navarro-Llobet, Ramon Agulló, Jordi Puig, Gustavo Gonzalez-Granadillo, Juan Mora Zamorano, and Ramon Romeu. 2021. Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach. Applied Sciences 11, 15 (2021). https://doi.org/10.3390/app11156699

[91] Candace Johnson. 2022. Drafting injustice: overturning Roe v. Wade, spillover effects and reproductive rights in context. Feminist Theory (August 2022), 14647001221114611. https://doi.org/10.1177/14647001221114611

[92] Colleen P. Judge, Tierney E. Wolgemuth, Megan E. Hamm, and Sonya Borrero. 2017. "Without bodily autonomy we are not free": exploring women's concerns about future access to contraception following the 2016 US presidential election. Contraception 96, 5 (November 2017), 370–377. https://doi.org/10.1016/j.contraception.2017.07.169

[93] Aditya Karandikar, Agnieszka Solberg, Alice Fung, Amie Y Lee, Amina Farooq, Amy C Taylor, Amy Oliveira, Anand Narayan, Andi Senter, and Aneesa Majid. 2023. Radiologists staunchly support patient safety and autonomy, in opposition to the SCOTUS decision to overturn Roe v Wade. Clinical imaging 93, (2023), 117–121.

[94] Robert N. Karrer. 2011. The Pro-Life Movement and Its First Years under "Roe." American Catholic Studies 122, 4 (2011), 47–72. https://doi.org/10.1353/acs.2011.0047

[95] WILL KENTON. 2021. Litigation Risk. Investopedia. Retrieved December 17, 2022 from https://www.investopedia.com/terms/l/litigation-risk.asp

[96] KFF Survey. 2019. Health Apps and Information Survey. Retrieved October 27, 2022 from https://www.kff.org/other/poll-finding/kff-health-apps-and-information-survey/

[97] Caroline Kitchener, Kevin Schaul, N. Kirkpatrick, Daniela Santamariña, and Lauren Tierney. 2022. Tracking the States Where Abortion Is Banned. The New York Times. Retrieved July 16, 2023 from https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html

[98] Thorin Klosowski. 2021. The State of Consumer Data Privacy Laws in the US (And Why It Matters). Wirecutter: Reviews for the Real World. Retrieved January 13, 2023 from https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

[99] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security 64, (2017), 122–134. https://doi.org/10.1016/j.cose.2015.07.002

[100] Yubo Kou, Xinning Gui, Yunan Chen, and Kathleen Pine. 2017. Conspiracy talk on social media: collective sensemaking during a public health crisis. Proceedings of the ACM on Human-Computer Interaction 1, CSCW (2017), 1–21. https://doi.org/10.1145/3134696

[101] Peter Krafft, Kaitlyn Zhou, Isabelle Edwards, Kate Starbird, and Emma S Spiro. 2017. Centralized, parallel, and distributed information processing during collective sensemaking. In (CHI '17), 2017, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 2976–2987. https://doi.org/10.1145/3025453.3026012
[102] Sandra Larsson. 2023. Examining Data Privacy and User Trust in Fertility-and Menstruation Technologies Using an Intersectional Feminist Perspective. Master's thesis. KTH Royal Institute of Technology, Stockholm, Sweden.
[103] Angela Lashbrook. 2022. How Private and Protected Is Virtual Reproductive Care? Consumer Reports. Retrieved January 14, 2023 from https://www.consumerreports.org/health-privacy/how-private-and-protected-is-virtual-reproductive-care-a2459174110/
[104] Karen EC Levy. 2014. Intimate surveillance. Idaho L. Rev. 51, (2014), 679.
[105] David Lyon. 2014. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society 1, 2 (July 2014), 2053951714541861. https://doi.org/10.1177/2053951714541861
[106] Lena Mamykina, Drashko Nakikj, and Noemie Elhadad. 2015. Collective sensemaking in online health forums. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15), 2015, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 3217–3226. https://doi.org/10.1145/2702123.2702566
[107] Kelly McCleary and Holly Yan. 2022. Abortion rights: Protests spread across the US after Supreme Court decision | CNN. Retrieved October 27, 2022 from https://www.cnn.com/2022/06/27/us/supreme-court-overturns-roe-v-wade-monday
[108] Nora Mcdonald and Nazanin Andalibi. 2023. "I Did Watch 'The Handmaid's Tale'": Threat Modeling Privacy Post-Roe in the United States. ACM Trans. Comput.-Hum. Interact. (March 2023). https://doi.org/10.1145/3589960
[109] Julianne McShane. 2022. Abortion providers face significant increase in violence, report finds. NBC News. Retrieved January 15, 2023 from https://www.nbcnews.com/news/us-news/abortion-providers-face-significant-increase-violence-report-finds-rcna35261
[110] Maryam Mehrnezhad and Teresa Almeida. 2021. Caring for Intimate Data in Fertility Technologies. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21), 2021, New York, NY, USA. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445132
[111] Maryam Mehrnezhad, Laura Shipp, Teresa Almeida, and Ehsan Toreini. 2022. Vision: Too Little Too Late? Do the Risks of FemTech Already Outweigh the Benefits? In Proceedings of the 2022 European Symposium on Usable Security (EuroUSEC '22), 2022, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 145–150. https://doi.org/10.1145/3549015.3554204
[112] Stefania Milan and Lonneke Velden. 2016. The Alternative Epistemologies of Data Activism. Digital Culture & Society 2, (December 2016). https://doi.org/10.14361/dcs-2016-0205
[113] Krys Mroczkowski, Colleen Ammerman, and Rembrand Koning. 2022. How Abortion Bans Will Stifle Health Care Innovation. Harvard Business Review. Retrieved November 21, 2022 from https://hbr.org/2022/08/how-abortion-bans-will-stifle-health-care-innovation
[114] Alexios Mylonas, Vasilis Meletiadis, Lilian Mitrou, and Dimitris Gritzalis. 2013. Smartphone sensor data as digital evidence. Computers & Security 38, (2013), 51–75. https://doi.org/10.1016/j.cose.2013.03.007
[115] Nancy A. Naples. 1996. A feminist revisiting of the insider/outsider debate: The "outsider phenomenon" in rural Iowa. Qualitative Sociology 19, 1 (March 1996), 83–106. https://doi.org/10.1007/BF02393249
[116] Farah Nayeri. 2021. Is 'Femtech' the Next Big Thing in Health Care? The New York Times. Retrieved October 23, 2022 from https://www.nytimes.com/2021/04/07/health/femtech-women-health-care.html
[117] ALFRED NG. 2022. Data brokers resist pressure to stop collecting info on pregnant people. POLITICO. Retrieved January 14, 2023 from https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988
[118] Sarah Ng, Shaowen Bardzell, and Jeffrey Bardzell. 2020. The Menstruating Entrepreneur Kickstarting a New Politics of Women's Health. ACM Trans. Comput.-Hum. Interact. 27, 4 (August 2020). https://doi.org/10.1145/3397158
[119] Jack Nicas. 2021. What Data About You Can the Government Get From Big Tech? The New York Times. Retrieved October 25, 2023 from https://www.nytimes.com/2021/06/14/technology/personal-data-apple-google-facebook.html
[120] Helen Nissenbaum. 2004. Privacy as contextual integrity. Wash. L. Rev. 79, (2004), 119.
[121] Helen Nissenbaum. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press. Retrieved from https://doi.org/10.1515/9780804772891
[122] Charles Ornstein. 2022. Federal Patient Privacy Law Does Not Cover Most Period-Tracking Apps. ProPublica. Retrieved January 15, 2023 from https://www.propublica.org/article/period-app-privacy-hipaa
[123] Ovia Health. 2023. Will I have irregular menstruation after a miscarriage? Ovia Health. Retrieved January 13, 2023 from https://www.oviahealth.com/guide/102445/pregnancy-loss-when-will-cycle-return-normal/
[124] Jessica A. Pater, Oliver L. Haimson, Nazanin Andalibi, and Elizabeth D. Mynatt. 2016. "Hunger Hurts but Starving Works": Characterizing the Presentation of Eating Disorders Online. In Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16), 2016, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 1185–1200. https://doi.org/10.1145/2818048.2820030
[125] Michael Quinn Patton. 1990. Qualitative evaluation and research methods. SAGE Publications, Inc.

[126] Michael Quinn Patton. 2014. Qualitative research & evaluation methods: Integrating theory and practice. Sage publications.
[127] Planned Parenthood. 2023. What are the Side Effects of In-Clinic Abortions? Retrieved January 13, 2023 from https://www.plannedparenthood.org/learn/abortion/in-clinic-abortion-procedures/what-can-i-expect-after-having-an-in-clinic-abortion
[128] Nicholas Proferes, Naiyan Jones, Sarah Gilbert, Casey Fiesler, and Michael Zimmer. 2021. Studying reddit: A systematic overview of disciplines, approaches, methods, and ethics. Social Media+ Society 7, 2 (2021), 20563051211019004. https://doi.org/10.1177/20563051211019004
[129] Dongxiao Qin. 2016. Positionality. In The Wiley Blackwell Encyclopedia of Gender and Sexuality Studies. 1–2. https://doi.org/10.1002/9781118663219.wbegss619
[130] Lauren Rankin. 2020. How an online search for abortion pills landed this woman in jail. Fast Company. Retrieved November 1, 2022 from https://www.fastcompany.com/90468030/how-an-online-search-for-abortion-pills-landed-this-woman-in-jail
[131] Marvin Rausand. 2013. Risk assessment: theory, methods, and applications. John Wiley & Sons.
[132] Reddit. 2020. Reddit's 2020 Year in Review - Upvoted. Retrieved October 7, 2022 from https://www.redditinc.com/blog/reddits-2020-year-in-review/
[133] Stavroula Rizou, Eugenia Alexandropoulou-Egyptiadou, and Konstantinos E. Psannis. 2020. GDPR Interference With Next Generation 5G and IoT Networks. IEEE Access 8, (2020), 108052–108061. https://doi.org/10.1109/ACCESS.2020.3000662
[134] Catherine Roberts. 2022. Period Tracker Apps and Privacy. Consumer Reports. Retrieved January 13, 2023 from https://www.consumerreports.org/health-privacy/period-tracker-apps-privacy-a2278134145/
[135] Celia Rosas. 2019. The Future is Femtech: Privacy and Data Security Issues Surrounding Femtech Applications. Business law journal 15, (2019), 319.
[136] Donna Rosato. 2020. What Your Period Tracker App Knows About You. Consumer Reports. Retrieved October 27, 2022 from https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you-a8701683935/
[137] Melody Rose. 2011. Pro-life, pro-woman? Frame extension in the American antiabortion movement. Journal of Women, Politics & Policy 32, 1 (2011), 1–27. https://doi.org/10.1080/1554477X.2011.537565
[138] Daniel Joseph Ryan and Gal Shpantzer. 2002. Legal Aspects of Digital Forensics. In Proceedings: Forensics Workshop, 2002.
[139] S. Das, W. K. Edwards, D. Kennedy-Mayo, P. Swire, and Y. Wu. 2021. Privacy for the People? Exploring Collective Action as a Mechanism to Shift Power to Consumers in End-User Privacy. IEEE Security & Privacy 19, 5 (October 2021), 66–70. https://doi.org/10.1109/MSEC.2021.3093135
[140] Safia Samee Ali. 2019. Missouri state health director tracked menstrual periods of Planned Parenthood patients. NBC News. Retrieved October 25, 2023 from https://www.nbcnews.com/news/us-news/missouri-health-director-tracked-menstrual-periods-planned-parenthood-patients-n1073701
[141] Rüdiger Schmitt-Beck. 2015. Bandwagon effect. The international encyclopedia of political communication (2015), 1–5. https://doi.org/10.1002/9781118541555.wbiepc015
[142] Justin Sherman. 2022. The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics. Default. Retrieved July 18, 2023 from https://www.lawfaremedia.org/article/data-broker-caught-running-anti-abortion-ads—-people-sitting-clinics
[143] Laura Shipp and Jorge Blasco. 2020. How private is your period?: A systematic analysis of menstrual app privacy policies. Proceedings on Privacy Enhancing Technologies 2020, (2020), 491–510.
[144] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14), 2014, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 2347–2356. https://doi.org/10.1145/2556288.2557421
[145] Susheela Singh and Gilda Sedgh. 2022. Global implications of overturning Roe v Wade. BMJ 378, (August 2022), o2025. https://doi.org/10.1136/bmj.o2025
[146] Ahmed Soliman, Jan Hafer, and Florian Lemmerich. 2019. A Characterization of Political Communities on Reddit. In Proceedings of the 30th ACM Conference on Hypertext and Social Media (HT '19), 2019, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 259–263. https://doi.org/10.1145/3342220.3343662
[147] Daniel J Solove. 2006. A taxonomy of privacy. University of Pennsylvania law review (2006), 477–564.
[148] Marie Louise Juul Søndergaard. 2020. Troubling Design: A Design Program for Designing with Women's Health. ACM Trans. Comput.-Hum. Interact. 27, 4 (August 2020). https://doi.org/10.1145/3397199
[149] Kayte Spector-Bagdady and Michelle M. Mello. 2022. Protecting the Privacy of Reproductive Health Information After the Fall of Roe v Wade. JAMA Health Forum 3, 6 (June 2022), e222656–e222656. https://doi.org/10.1001/jamahealthforum.2022.2656
[150] Anna Cinzia Squicciarini, Mohamed Shehab, and Federica Paci. 2009. Collective Privacy Management in Social Networks. In Proceedings of the 18th International Conference on World Wide Web (WWW '09), 2009, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 521–530. . https://doi.org/10.1145/1526709.1526780

[151] Stacey D, Légaré, F, Lewis, K, Barry, MJ, Bennett, CL, Eden, KB, Holmes-Rovner, M, Llewellyn-Thomas, H, Lyddiatt, A, Thomson, R and L Trevena. 2017. Decision aids for people facing health treatment or screening decisions. Cochrane Database of Systematic Reviews 4 (2017). https://doi.org/10.1002/14651858.CD001431.pub5

[152] State of California Department of Justice Office of The Attorney General. 2022. Attorney General Bonta Emphasizes Health Apps' Legal Obligation to Protect Reproductive Health Information. State of California - Department of Justice - Office of the Attorney General. Retrieved April 15, 2023 from https://oag.ca.gov/news/press-releases/attorney-general-bonta-emphasizes-health-apps-legal-obligation-protect

[153] Jennifer Jiyoung Suh, Miriam J. Metzger, Scott A. Reid, and Amr El Abbadi. 2018. Distinguishing Group Privacy From Personal Privacy: The Effect of Group Inference Technologies on Privacy Perceptions and Behaviors. Proc. ACM Hum.-Comput. Interact. 2, CSCW (November 2018). https://doi.org/10.1145/3274437

[154] Frost & Sullivan. 2018. Femtech—Time for a Digital Revolution in the Women's Health Market. Frost & Sullivan. Retrieved May 5, 2023 from https://www.frost.com/frost-perspectives/femtechtime-digital-revolution-womens-health-market/

[155] Humphrey Taylor. 2003. Most people are "privacy pragmatists" who, while concerned about privacy, will sometimes trade it off for other benefits. The Harris Poll 17, 19 (2003), 44.

[156] Linnet Taylor. 2017. Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World. In Group Privacy: New Challenges of Data Technologies, Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds.). Springer International Publishing, Cham, 13–36. https://doi.org/10.1007/978-3-319-46608-8_2

[157] Linnet Taylor, Luciano Floridi, and Bart van der Sloot. 2017. Introduction: A New Perspective on Privacy. In Group Privacy: New Challenges of Data Technologies, Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds.). Springer International Publishing, Cham, 1–12. https://doi.org/10.1007/978-3-319-46608-8_1

[158] The Associated Press. 2022. Abortion ruling prompts variety of reactions from states. AP NEWS. Retrieved October 27, 2022 from https://apnews.com/article/supreme-court-abortion-ruling-states-a767801145ad01617100e57410a0a21d

[159] The Editors of Encyclopaedia Britannica. 2022. Roe v. Wade | Summary, Origins, & Influence | Britannica. Retrieved October 26, 2022 from https://www.britannica.com/event/Roe-v-Wade

[160] Ida Tin. 2016. The rise of a new category: Femtech. Retrieved January 15, 2023 from https://helloclue.com/articles/culture/rise-new-category-femtech

[161] Ariana M Traub, Kellen Mermin-Bunnell, Priyasha Pareek, Sonya Williams, Natalie B Connell, Jennifer F Kawwass, and Carrie Cwiak. 2022. The implications of overturning Roe v. Wade on medical education and future physicians. The Lancet Regional Health–Americas 14, (2022).

[162] Anupriya Tuli, Surbhi Singh, Rikita Narula, Neha Kumar, and Pushpendra Singh. 2022. Rethinking Menstrual Trackers Towards Period-Positive Ecologies. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22), 2022, New York, NY, USA. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3491102.3517662

[163] Jessica Vitak. 2012. The impact of context collapse and privacy on social network site disclosures. Journal of broadcasting & electronic media 56, 4 (2012), 451–470.

[164] Jessica Vitak, Nicholas Proferes, Katie Shilton, and Zahra Ashktorab. 2017. Ethics regulation in social computing research: Examining the role of institutional review boards. Journal of Empirical Research on Human Research Ethics 12, 5 (2017), 372–382.

[165] Yu-Chih Wei, Wei-Chen Wu, Gu-Hsin Lai, and Ya-Chi Chu. 2020. pISRA: privacy considered information security risk assessment model. The Journal of Supercomputing 76, 3 (March 2020), 1468–1481. https://doi.org/10.1007/s11227-018-2371-0

[166] Karl E Weick. 1995. Sensemaking in organizations. Sage.

[167] Cynthia O'Donoghue Wilde-Detmering Joana Becker, Friederike. 2022. CJEU rules on interpretation of EU GDPR special categories of data. Technology Law Dispatch. Retrieved April 16, 2023 from https://www.technologylawdispatch.com/2022/08/privacy-data-protection/cjeu-rules-on-interpretation-of-eu-gdpr-special-categories-of-data/

[168] Ben Wolford. 2018. What is GDPR, the EU's new data protection law? GDPR.eu. Retrieved December 20, 2022 from https://gdpr.eu/what-is-gdpr/

[169] Lauren Worsfold, Lorrae Marriott, Sarah Johnson, and Joyce C Harper. 2021. Period tracker applications: What menstrual cycle information are they giving women? Women's Health 17, (2021), 17455065211049905.

[170] Yuxi Wu, W. Keith Edwards, and Sauvik Das. 2022. "A Reasonable Thing to Ask For": Towards a Unified Voice in Privacy Collective Action. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22), 2022, New York, NY, USA. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3491102.3517467

[171] Sijia Xiao, Coye Cheshire, and Amy Bruckman. 2021. Sensemaking and the Chemtrail Conspiracy on the Internet: Insights from Believers and Ex-believers. Proceedings of the ACM on Human-Computer Interaction 5, CSCW2 (2021), 1–28.

[172] Cat Zakrzewski, Pranshu Verma, and Claire Parker. 2022. Police used texts, web searches for abortion to prosecute women - The Washington Post. Retrieved November 1, 2022 from https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/

[173] Christoph Zott, Raphael Amit, and Lorenzo Massa. 2011. The business model: recent developments and future research. Journal of management 37, 4 (2011), 1019–1042.

APPENDIX

Appendix A. List of the subreddits where the posts we collected were published

Subreddit	Count	Subreddit	Count
amipregnant	116	h3h3productions	1
TwoXChromosomes	97	Hasan_Piker	1
Periods	93	Health	1
birthcontrol	73	Health2020	1
TryingForABaby	54	helpingwomen	1
WitchesVsPatriarchy	48	helpme	1
SafeSexPH	46	HelpMeFind	1
sex	36	HormoneFreeMenopause	1
pregnant	33	HotWifeLifestyle	1
PMDD	31	HoustonClassifieds	1
AskDocs	30	Hypothyroidism	1
dirtypenpals	25	hysterectomy	1
PCOS	25	imlovelylayla	1
DirtyChatPals	23	IMPORTANTANONUCMENTS	1
WomensHealth	20	impregnation	1
BabyBumps	19	Infidelity	1
TFABLinePorn	18	Inito	1
childfree	17	inthenews	1
AppleWatch	16	iOSBeta	1
obgyn	16	Iowa	1
privacy	15	iphone	1
prochoice	15	JasmyToken	1
AskWomen	14	javahelp	1
AutoNewspaper	14	Jcore	1
technology	14	jimmydoreshow	1
Advice	13	kansascity	1
adhdwomen	12	kpopthoughts	1
ATEEZ	12	LeanPCOS	1
TheGirlSurvivalGuide	12	learnprogramming	1
businesstalkdaily	11	legaladvice	1
FAMnNFP	11	legaladviceofftopic	1
relationship_advice	11	Liberal	1
videosUSATODAYauto	11	Libertarian	1
WatchesVaginalPreppers	11	MachineLearning	1
weightroomvideos	11	madlad	1
whatsnewtodayWatches	11	maletime	1
whiteknightingweightroom	11	MaliciousCompliance	1
WhitePeopleTwitterwhatsnewtoday	11	mariokart	1
wildlandwhiteknighting	11	marketpredictors	1
witchcraftWhitePeopleTwitter	11	May2023BumpGroup	1
wlswildland	11	MCAS	1
WomenHealthCarewitchcraft	11	medicalmedium	1

WomenHealthTreatmentswls	11	medicine	1
WomenInNewsWomenHealthCare	11	mexico	1
worldnewsindexWomenHealthTreatments	11	mildlyinfuriating	1
YoutubeGossip_NewsWomenInNews	11	mildlyinteresting	1
YSKworldnewsindex	11	missouri	1
zoloftYoutubeGossip_News	11	moderatelygranolamoms	1
farkYSK	11	mohsana700	1
FDroidUpdateszoloft	11	Mom	1
FemaleAntinatalismfark	11	MomForAMinute	1
feminismsFDroidUpdates	11	Money	1
floridaFemaleAntinatalism	11	motherinlawsfromhell	1
forcedbreedingfeminisms	11	namenerds	1
fossflorida	11	NashvilleJobs	1
FTMMenforcedbreeding	11	newbrunswickcanada	1
FTMOver30foss	11	NewParents	1
futureofsexFTMMen	11	newsfeedmedia	1
gamingFTMOver30	11	NewsfromNowhere	1
gaytransguysfutureofsex	11	newsintechnology	1
GERDgaming	11	newslive	1
GEVOtickergaytransguys	11	NewsOfTheWeird	1
girlsGERD	11	Newsoku_L	1
GirlSurvivalGuideGEVOticker	11	NoContract	1
abortion	10	nordvpn	1
NoStupidQuestions	10	NotHowGirlsWork	1
AskReddit	9	Notion	1
news	9	Novavax_vaccine_talk	1
OutOfTheLoop	9	NurseAllTheBabies	1
TFABChartStalkers	9	NYPOSTauto	1
TrollXChromosomes	9	nytimes	1
NewsfeedForWork	8	NZHauto	1
Nexplanon	8	ObsidianMD	1
apple	7	OCD	1
hackerdigest	7	offmychest	1
LifeProTips	7	OffMyChestPH	1
tryingtoconceive	7	okdemocrats	1
ttcafterloss	7	oneanddone	1
askwomenadvice	6	onguardforthee	1
Healthyhooha	6	opensource	1
News_IT	6	orlando	1
politics	6	ostomy	1
relationships	6	PaidStudyHub	1
women	6	PaidSurveys	1
breakingmom	5	Paranormal	1
Endo	5	Parenting	1
Feminism	5	Philippines	1
fitbit	5	planbshow	1
lineporn	5	Political_Revolution	1
Miscarriage	5	PoliticalOpinions	1

TheColorIsOrange	5	PoliticalVideo	1
TooAfraidToAsk	5	PoliticalVideos	1
YouShouldKnow	5	PopcornPundits	1
applehelp	4	Pregnantroleplay	1
April2023BumpGroup	4	PrepperIntel	1
badwomensanatomy	4	preppers	1
beyondthebump	4	Proprotection	1
CopperIUD	4	propublica	1
endometriosis	4	PutACupInIt	1
medical_advice	4	RadicalLegalAdvice	1
menstruation	4	raisedbynarcissists	1
PaidStudies	4	RandomThoughts	1
sexquestions	4	rant	1
TTC_PCOS	4	realtech	1
viral	4	Rivian	1
waiting_to_try	4	RoevWadeCelebration	1
ADHD	3	RoevWadeUndergroundRR	1
AmItheAsshole	3	sandiego	1
auntienetwork	3	SapphoAndHerFriend	1
CasualConversation	3	SASSWitches	1
CitadelLLC	3	selfhosted	1
ClashRoyale	3	SeveralGrass	1
conspiracy	3	sexed	1
GUARDIANauto	3	sexstories	1
hypeurls	3	sexualassault	1
IVF	3	shortcuts	1
knowyourshit	3	Sims4	1
medical	3	sleep	1
Mirena	3	SmashingSecurity	1
Mommit	3	StallmanWasRight	1
MtF	3	StealthFTM	1
News_HealthBiotech	3	StealthTransgender	1
NoFilterNews	3	stilltrying	1
nsfw_roleplay	3	StLouis	1
PregnancyAfterLoss	3	StockMarket	1
PrivacyGuides	3	stupidpol	1
queerception	3	supremecourt	1
Rants	3	surfshark	1
RedditSample	3	surgicalmenopause	1
StonkFeed	3	TableauTheInternet	1
tech	3	TabooRolePlaynsfw	1
TranscribersOfReddit	3	technewslive	1
TrendingQuickTVnews	3	TestosteroneKickoff	1
TwoXSex	3	The__Verge	1
196	2	theconversation_au	1
Abortiondebate	2	TheHandmaidsTale	1
Anxiety	2	TheJanesNextGen	1
AskFeminists	2	thesims	1
AskWomenOfColorOver30	2	theworldnews	1
AskWomenOver30	2	tientien2022	1

Birthcontroltalk	2	tirwander	1
boringdystopia	2	TooAfraidToAskboutSex	1
BPD	2	TopConspiracy	1
bulletjournal	2	TopInteresting	1
CNNauto	2	TopLifeTips	1
CyberNews	2	ToR_Archive	1
DeadBedrooms	2	torchsecuritynet	1
drumcorps	2	traaaaaaannnnnnnnnns	1
EroticRolePlay	2	trans	1
explainlikeimfive	2	trees	1
ftm	2	trollingforababy	1
IllegalLifeProTips	2	TrollYChromosome	1
IUD	2	TrueOffMyChest	1
LateStageCapitalism	2	TrueTrueReddit	1
LATIMESauto	2	Trying2conceive	1
laughingzebra	2	tryingforanother	1
loseit	2	twitter_read	1
MacroFactor	2	TwoXADHD	1
March2023BumpGroup	2	TwoXPreppers	1
miband	2	girls	1
moreplatesmoredates	2	GirlSurvivalGuide	1
nursing	2	Anxietyhelp	1
Nuvaring	2	AnythingGoesNews	1
NYTauto	2	AnythingOntario	1
ouraring	2	app	1
paidstudy	2	ArizonaLeft	1
PlanBs	2	ask	1
PlannedParenthood	2	ask_transgender	1
PMDDSharing	2	AskAstrologers	1
PMS	2	AskMtFHRT	1
politicly	2	AskNYC	1
PregnancyUK	2	asktransgender	1
prolife	2	assholedesign	1
redscarepod	2	astrology	1
SatanicTemple_Reddit	2	BacterialVaginosis_	1
SluttyConfessions	2	BadChoicesGoodStories	1
technews	2	BearableApp	1
teenagers	2	BenignExistence	1
tifu	2	BestofRedditorUpdates	1
UnethicalLifeProTips	2	Biohackers	1
venting	2	bjj	1
weddingplanning	2	blackladies	1
30PlusSkinCare	1	BlackTransgender	1
49ers	1	BreakingPoints	1
75HARD	1	breastfeeding	1
ABoringDystopia	1	breastfeedingsupport	1
AbusiveLPT	1	BreedingStories	1
Accutane	1	bupropion	1
adenomyosis	1	CalyxOS	1
ADHDmeds	1	canada	1

AdultADHDSupportGroup	1	CashApps	1
AdviceAnimals	1	Catholicism	1
AITAH	1	CautiousBB	1
alasjuicy	1	ChurchOfSuffrage	1
aliceandfernsnark	1	CKsTechNews	1
alltechnewz	1	collapse	1
AmazonMusic	1	collapse_wilds	1
AmIBeingTooSensitive	1	collapze	1
AmITheAngel	1	CommercialClub	1
Anarchism	1	dumbphones	1
Android	1	EatingDisorders	1
android_devs	1	EctopicSupportGroup	1
androidapps	1	endocrinology	1
androiddev	1	esist	1
antiassholedesign	1	Exvangelical	1
antiwork	1	GLOBEauto	1
community	1	gravesdisease	1
conspiracy_commons	1	DailyShow	1
ConstipationAdvice	1	Daylio	1
CrazyIdeas	1	DemocraticUnderground	1
CRedit	1	DID	1
daddit	1	digitalessay	1

Received July 2023; revised October 2023; accepted November 2023.