This is a pre-print of an article accepted at ACM SIGCHI Conference on Computer-Supported Cooperative Work & Social Computing for 2025. A formal citation will be available by May 2025. However, for now, please cite as:

Nadia Karizat, Nora McDonald, and Nazanin Andalibi. 2025. *Laboring Towards Sociotechnical Reproductive Privacy in a Post-Roe United States: Identities, Technologies, and Actors Implicated in Reproductive Privacy.* Proceedings of the ACM on Human Computer Interaction, CSCW, forthcoming April 2025.

Laboring Towards Sociotechnical Reproductive Privacy in a Post-Roe United States: Identities, Technologies, and Actors Implicated in Reproductive Privacy

NADIA KARIZAT, University of Michigan, USA
NORA MCDONALD, George Mason University, USA
NAZANIN ANDALIBI, University of Michigan, USA

The overturning of *Roe v. Wade* in 2022 by the U.S. Supreme Court in *Dobbs v. Jackson* exposed and exacerbated existing gaps in reproductive privacy. In the post-Roe era, aggressive surveillance by both government and private entities has made real and heightened concerns about privacy violations for people capable of pregnancy (PCOP). We investigate PCOPs' reproductive privacy concerns and the strategies they use to address these concerns post-Roe. We conducted semi-structured interviews with 18 adult cisgender women and transgender men in the U.S. Our findings show that for PCOPs, privacy risks are both persistent and anomalous, imposing what we conceptualize as *reproductive privacy labor*, a type of safety and data work that is, to them, both necessary and exhausting. We introduce the conceptual framework *Sociotechnical Reproductive Privacy*, outlining the relationships between actors, technologies, and identities that are implicated in the many contexts of reproductive privacy vulnerabilities post-Roe. We conclude with considerations for research and design, and explore the utility of approaches like refusal and regulation (e.g., technical, policy) in promoting sociotechnical reproductive privacy. This research underscores the urgent need to address the intersection of reproductive rights, privacy, and technology, offering insights into how affected individuals navigate and manage their reproductive health decisions in an increasingly surveilled sociotechnical landscape.

CCS Concepts: • **Human-centered computing** → *Empirical studies in HCI*; **Empirical studies in HCI**; • **Security and privacy** → *Human and societal aspects of security and privacy*; *Privacy protections*; • **Social and professional topics** → *Gender*.

Additional Key Words and Phrases: Intimate Data; Privacy; Privacy Risk; Privacy Labor; Privacy Strategies; Reproductive Health; Reproductive Privacy Labor; Reproductive Rights; Sociotechnical Reproductive Privacy; Safety Work; Data Work; Intimate Privacy

1 INTRODUCTION

In 2022, the U.S. Supreme Court's decision in *Dobbs v. Jackson* [2] overturned the court's ruling in *Roe v. Wade* (1973). Roe granted women the right to obtain an abortion under the supervision of a licensed physician and affirmed the privacy of one's decisions regarding abortion, procreation, and child-rearing as protected by the 14th amendment [90]. Before and *and* now, after *Roe*, the reproductive

Authors' addresses: Nadia Karizat, nkarizat@umich.edu, University of Michigan, Ann Arbor, Michigan, USA; Nora Mcdonald, nmcdona4@gmu.edu, George Mason University, Fairfax, Virginia, USA; Nazanin Andalibi, andalibi@umich.edu, University of Michigan, Ann Arbor, USA.

ACM 0004-5411/2025/8-ART111
https://doi.org/XXXXXXX.XXXXXXX

capacity of people capable of pregnancy (PCOP) has been a site of state-sanctioned policing and surveillance [37], with the U.S. government's long history of implementing policy threatening access to reproductive healthcare and reproductive privacy [72]. We refer to reproductive privacy as *privacy pertaining to individuals' reproductive decisions and experiences* (e.g., decisions to (not) have an abortion, to (not) use contraception, (not) be pregnant, or (not) manage infertility). What is unique to recent threats to reproductive privacy in the Post-Roe era are the massive amounts of retrospective data (e.g., location, texts, images, electronic health records, online behavior) collected about the public that can be used in efforts to control, police, and criminalize reproductive health experiences (e.g., abortion, pregnancy, miscarriage) [4, 9, 25, 91]. Given the heightened stakes associated with reproductive privacy post-Roe, recent Human-Computer Interaction (HCI) and social computing scholars are examining how individuals most affected are thinking about their privacy [16, 26] and the way this thinking intersects with different contexts of risk [57]. Building on this past work, our study provides an updated and in-depth examination of PCOPs' reproductive privacy concerns and mitigation strategies.

Through semi-structured interviews with 18 adults consisting of cisgender women and transgender men in the U.S., we found that participants perceived a lack of control over their reproductive health information and worried about the potential legal and social implications if their data were obtained and acted on by individuals or institutions with power over their lives. To manage these reproductive privacy concerns, participants described several technology strategies such as efforts to deliberately modify, obfuscate [13] or otherwise reduce one's reproductive health-related digital footprints. To conceptualize the various kinds of labor participants engaged in to protect their privacy, we introduce the term ***reproductive* privacy labor**—which we view as a type of safety work [48] and data work [66]—to describe the sociotechnical labor individuals perform to manage their reproductive privacy, which may or may not lead to successful privacy protection. Our findings culminate in the conceptual framework of ***sociotechnical reproductive privacy***, which we use to describe privacy pertaining to data that may be deemed as relevant to, or as evidence of individuals' reproductive decisions and experiences that may be both threatened *and* protected by the relationships between actors—human and not—, technology, and identity. Building on prior work [4, 26, 54, 57, 59, 60, 62], outlining this concept promotes a meaningful tool for thinking about the overlapping social and personal health risks, as well as the technical complexities, that define this dynamic and multifaceted landscape. Sociotechnical reproductive privacy is thus presented as a concept for future exploration and empirical evaluation.

A Note on Terminology. Reproductive health is often equated with "women's health" where "women" equates to cisgender women, including in HCI [49]. However, aligning with [49, 71] we view reproductive health as inclusive of not only cisgender women, but also men, non-binary individuals, and transgender people. As such, we opt for gender-neutral, descriptive language, such as people capable of pregnancy (PCOP), individuals with reproductive systems capable of pregnancy, and so on. However, when we reference prior works, policies, or historical contexts organized around normative notions of *women*, we echo their terminology unless otherwise stated.

2 RELEVANT WORK

2.1 The Dismantling of Roe v. Wade and Increased Policing of Reproductive Healthcare and Experiences in the U.S.

The 1973 U.S. Supreme Court decision in *Roe v. Wade* decriminalized abortions nationwide by granting the right to abortions with the consultation of a licensed physician, *and* argued the right to privacy extended to abortions [90]. However, it did not prevent state governments from introducing barriers aimed at discouraging abortion (e.g., mandatory waiting periods, requiring an ultrasound)

or guaranteeing all who wanted to receive an abortion would be able to access it (e.g., banning public insurance coverage) [34, 40]. Nonetheless, *Roe v. Wade* was a turning point for reproductive rights, granting people the federal right to end their pregnancy, including for exceptions (e.g., rape, incest, mother's life at risk) that had not existed in some states. [1] In 2022, however, the right to an abortion was lost with the *Dobbs v. Jackson Women's Health Organization* decision [2] leaving the right to access abortions for state governments to determine. Notably, since 2022, concern over proposed or passed legislation targeting other types of reproductive healthcare (e.g., IVF, contraception) or experiences has grown [33, 55, 76, 78].

Following the Dobbs decision, there has been a rise in the policing (de jure and de facto) [44] of reproductive healthcare, reproductive healthcare professionals, organizations, and PCOPs [17, 28, 43, 55, 79, 91]. People who have experienced miscarriages [70, 80], abortions, or assisted others in accessing an abortion [28, 29] have faced prosecution after being accused of violating their State's laws. While law enforcement and other authorities have been involved in these prosecutions, individuals' reproductive healthcare experiences (e.g., miscarriages, abortions) or intentions (e.g., seeking out an abortion) have also been reported by those in their social networks to law enforcement at times [17]. Within this increased policing of reproductive healthcare at multiple levels, individuals' information and behavior (e.g., online data, geolocation, or chat history) have been used as both evidence to prosecute or tools to enforce restrictive laws [15, 63, 91].

We situate our study within this Post-Roe context with increased policing of reproductive health, as well as the legacy of reproductive health surveillance in the U.S. in which the policing of women and PCOPs has been paramount, which we turn to next.

2.2 A Brief Overview of Privacy Challenges in the U.S. Reproductive Policy History

With the fall of *Roe v. Wade* in 2022, growing threats to reproductive freedoms [55], and recent instances of state-sanctioned reproductive health surveillance [15, 91**?**], it is important to recognize that the U.S. has a long history of implementing policy that poses threats to accessing reproductive healthcare, and reproductive privacy via surveillance [72, 81, 90]. Starting in the late 19th century, Congress passed the Comstock Law [77] effectively banning the distribution of "any article or thing designed or intended for the prevention of conception or procuring an abortion" [77] permitting officials to surveil any letters or parcels moving through the U.S. postal service [72]. While the law's criminalization of contraception was overturned by the 1965 Supreme Court's *Griswold v. Conneticut* decision [38], it set a precedent for State surveillance of reproductive health care and PCOPs' data.

PCOPs' privacy has historically been vulnerable to pro- and anti-natalist public policies that aimed to govern reproductive capacity for some based on class and race. Desires to maintain the 'white' racial majority in the U.S. prompted policy that infringed on the privacy of middle class white women and their right to (not) have children via measures like the Comstock law [72, 77]. Racist panic about the provision of welfare to 'poor' and 'irresponsible' women enabled state policies that allowed for surveillance of mothers deemed 'illegitimate' (e.g., based on race, based on class) [72]. Through some States conditioning welfare assistance, it became legal for fraud teams to surveil mothers on welfare, demand entry into one's home if they suspected a man was present, and police the sexuality and child-rearing of poor women [8, 52]. As recently as the 1990s, some states attempted to make contraception mandatory for PCOPs to access welfare benefits [72]. These historical policies are examples of how race and class shaped policy that violated PCOP's privacy.

[1]We recognize that there are many reasons why a person might choose or determine they need an abortion. Here, we are intentional with our language to avoid perpetuating what Katie Watson refers to as an *Abortion masterplot* that abortion is *always* a difficult decision. While it may be difficult for some in certain contexts, for others, it might be an "ordinary" healthcare procedure [90].

Continuing into the present day, States' punitive policies and legislation criminalize motherhood and pregnancy, and deny privacy and reproductive autonomy to PCOPs—disproportionately impacting PCOPs of color and those of lower socioeconomic status [35, 37]. For example, the existence of abortion deserts—cities with the nearest abortion clinic 100 miles or farther away—are a direct result of state policies that restrict access to critical reproductive healthcare and increase the logistical, financial, and emotional hurdle a PCOP has to navigate to access these services [18]. Opportunities exist for administrations and policy-makers to enforce more stringent restrictions on abortion and other reproductive healthcare [32]. We see this with recent legislating challenging the legality of shipping abortion medication (e.g., mifepristone) via mail and telemedicine [19], as well as the chipping away at *Roe v. Wade* between 1973 and 2022 that introduced over 1,000 restrictions (e.g., 6-week bans [42], reason-based bans [31]) across States to limit access to abortions [30, 69].

While we do not provide an all-inclusive account of policy and surveillance threats to reproductive privacy in the U.S. here, we demonstrate that privacy violations of PCOPs have been an ongoing and lawful part of history in the U.S. way before the dismantling of Roe v. Wade. And yet, the fall of *Roe v. Wade* and growing threat to reproductive health care [55] in light of new surveillance technology has heightened the stakes of reproductive privacy for PCOPs. Legal scholars concur that the advancement of "modern technologies directed toward [the] investigation of individuals" [25] make it possible to gather up vast swaths of intimate digital data retrospectively (e.g., years of location and purchase history, social media and other communications) and has fundamentally changed the nature of the threat to reproductive privacy.

2.3 Reproductive Privacy in Sociotechnical Contexts

Digital privacy within the realm of reproductive health has garnered increasing attention within the fields of HCI and social computing [4, 16, 26, 54, 57, 59–62]. With the explosion of technologies datafying reproductive capacity and large swaths of intimate data emerging, considering implications for intimate privacy is critical for both data subjects and society as a whole [4].

Research of FemTech (e.g., female-oriented technologies such as menstrual and fertility tracking apps [MFTA]) in the U.K. has demonstrated that people understand data collected by these intimate devices and apps is sensitive and perceive privacy risks, but are unclear of exactly how this data is managed, and feel unequipped to protect themselves against security and privacy risks [60]. Post-Roe, in the U.S., people feel similarly helpless to mitigate the risk of their data from period tracking apps being used against them [16]. These concerns are legitimate, as period tracking apps collect a wide range of sensitive data (e.g., sex life, location, menstrual cycle) and their privacy policies often permit data sharing with authorities [26, 59]. Yet much of FemTech remains unregulated [62] and pushes the responsibility to assess and manage reproductive privacy risks onto individuals.

Other HCI research in this space takes a more holistic perspective on technologies that can implicate reproductive privacy than those covered in FemTech studies. For example, following the reversal of Roe v. Wade, McDonald and Andalibi observed that individuals began implementing diverse privacy strategies with their technology usage in anticipation of potential intrusions that could expose their reproductive health decisions (e.g., abortion or terminating a pregnancy) in undesirable ways [57]. Notably, they found that individuals facing complex circumstances, such as high reproductive risk or uncertain legislative environments, employed low- and high-tech strategies to manage reproductive privacy risks [57].

With an understanding of how reproductive privacy has been a contentious issue in the U.S., and that recent legislation has contributed to an increased policing of reproductive healthcare and experiences, it is clear that reproductive privacy is an important context for social computing and HCI researchers to grapple with. While much prior HCI work has focused on reproductive privacy in the context of period tracking apps [4, 26, 54, 59, 60, 62], we build on these works and join McDonald

and Andalibi who consider a wider breadth of technologies and actors implicated in managing reproductive privacy—as the information produced by and collected from technologies (beyond traditional FemTech) pose a risk to PCOPs and their ability to access reproductive healthcare as they wish [57]. In this study, we add to the literature by deepening our investigation of perceived technology risk and mitigation strategies post-Roe and contributing frameworks for understanding risk more holistically.

Considering the literature reviewed here, we address the following research questions in the context of the United States post-Roe:

(1) What are the perceived reproductive privacy concerns among PCOPs?
(2) How do PCOPs mitigate their reproductive privacy concerns with technology strategies?

3 METHODS

3.1 Recruitment

We recruited participants as part of a larger study about the intersections of privacy, health, and technology. We conducted semi-structured interviews (*N=18*) with adult cisgender women and transgender men in the U.S. who reported reproductive health as personally relevant (minimum eligibility criteria). We recruited participants using a recruitment firm. Potential participants completed a screening survey to assess eligibility for the interviews. The screening survey received 303 responses, of which 109 met the minimum eligibility criteria. We invited 60 respondents to interviews. Of the 32 participants who expressed interest, 18 completed interviews during October and November 2024. We stopped data collection when we achieved data saturation, noting no additional codes during the coding process and no new themes in analytical memos.

3.2 Screening Survey

We directed respondents interested in participating in the study to Qualtrics to fill out a screening survey—we asked them to report their racial or ethnic origin, gender identity, sexual orientation, if they self-identify as low-income, the types of health-related information that are relevant to them (e.g. mental health, reproductive health), the state in the U.S. they reside in, and state(s) in the U.S. they've lived in previously.

Respondents were eligible for interviews if they selected reproductive health as a type of health information relevant to them. The recruitment firm allowed for filtering of potential participants by age and country of residence, so only participants over the age of 18 and who currently lived in the U.S. filled out the screening.

We did not include questions in the screening survey explicitly asking about privacy concerns *or* reproductive health and associated laws. This was because we were aware that participants might share sensitive information with us, and we aimed to mitigate risks to participants and their data.

3.3 Interview Participants and Protocol

We invited participants to participate in interviews based on their responses to the screening survey. We over-sampled for a diverse range of participants along the axes of location, race, sexual orientation, gender, and socioeconomic status. Table 1 provides information about participants' self-reported demographics. Of the participants, 38% were white/caucasian, 88% were women, and 61% were between 34 and 18 years of age. 44% of the participants were LGBTQ, and 61% were not low-income. Additionally, 55% of the participants lived in states with restrictive or most restrictive abortion policies as identified in [40]. To protect participants' privacy, we have listed the description

Pseudonym	Age	Race	Gender	Sexual Orientation	Education	Low Income?	State's Abortion Policies
Valerie	25-34	White/Caucasian	Woman	Bisexual	College	Yes	Most Restrictive
Morgan	35-44	White/Caucasian	Woman	Heterosexual/Straight	Some College	Other	Most Restrictive
Susanna	45-54	Asian or Pacific Islander	Woman	Heterosexual/Straight	College	No	Protective
Daniela	45-54	Hispanic or Latino/Latina/Latinx	Woman	Heterosexual/Straight	High School	Yes	Most Restrictive
Noor	25-34	American Indian/Native American or Alaska Native, Black or African American, White/Caucasian, Hispanic or Latino/Latina/Latinx	Man/ Transgender Abinary TransMasc	Queer	Some College	Yes	Most Restrictive
Lauren	25-34	Asian or Pacific Islander	Woman	Heterosexual/Straight	Some Graduate School	No	Protective
Yasmine	25-34	Black or African American, White/Caucasian	Woman	Queer	Graduate Degree	No	Protective
Roxana	35-44	White/Caucasian	Woman	Heterosexual/Straight	College	No	Most Restrictive
Aliza	25-34	Asian or Pacific Islander	Woman	Heterosexual/Straight	College	Yes	Protective
Naomi	35-44	Hispanic or Latino/Latina/Latinx	Woman	Bisexual	Graduate Degree	Not Sure	Restrictive
Alya	25-34	Asian or Pacific Islander	Woman	Heterosexual/Straight	Graduate Degree	No	Protective
Darcy	25-34	Hispanic or Latino/Latina/Latinx	Woman	Bisexual	Some College	No	Restrictive
Julie	35-44	White/Caucasian	Woman	Heterosexual/Straight	College	No	Restrictive
Shauna	45-54	Black or African American	Woman	Heterosexual/Straight	Graduate Degree	No	Restrictive
Cheyenne	25-34	Asian or Pacific Islander	Woman	Heterosexual/Straight	College	No	Protective
Serena	25-34	White/Caucasian	Woman	Heterosexual/Straight	Graduate Degree	No	Most Restrictive
Kai	18-24	White/Caucasian	Man/Transgender	Bisexual	College	Yes	Protective
Simone	25-34	Black or African American	Woman	Heterosexual/Straight	Some Graduate School	No	Protective

Table 1. Participant Demographics. Instead of reporting participants' locations (e.g., State of Residency), we chose to provide information about their reported State's Abortion Policies. These are organized by the Guttmacher institute's scores of States' Abortion Policies based on a State's number of supportive or restrictive abortion measures in effect [40].

of the state's abortion policies (e.g. restrictive, protective) as categorized by the Guttmacher Institute [40] in place of participants' self-reported state of residency. [2]

The protocol (Appendix A) led participants (without explicit reference to Roe) through questions relating to their reproductive privacy concerns and how these concerns have shaped the ways they used a variety of technologies. We also asked participants about their familiarity with, and understanding of, laws governing reproductive health and health privacy in their state. If Roe hadn't naturally come up in interviews at that point, that question frequently prompted participants to reference Roe or other legislation targeting reproductive health. We chose to prioritize participants' understandings and familiarity with legislation at the time of interviews, as opposed to providing a 'correct' awareness of specific state law (e.g., abortion ban) or legislative events (e.g., the overturning of Roe v. Wade).

The first author conducted interviews using Zoom's voice calling services. Interviews lasted from 20 to 88 minutes (average = 56 minutes). Participants were compensated $50 for completing the interview.

3.4 Data Analysis

The first author wrote memos after each interview to keep track of emerging themes. Interviews were audio recorded, transcribed using a local open-source transcribing software, and, once completely manually redacted, coded using qualitative coding software.[3] The first author open-coded all interviews [22], noting when no new codes emerged for when data saturation was reached. At

[2]Guttmacher Institute uses seven levels to describe abortion policies in the U.S.: Most restrictive; Very restrictive; Restrictive; Some restrictions/protections; Protective; Very protective; Most protective. Guttmacher Institute explains that these assigned levels for a state's abortion policies are the product of assessing *"20 types of abortion restrictions—including gestational duration bans, waiting periods, insurance coverage bans and medication abortion restrictions—and approximately 10 protective policies—including state constitutional protections, abortion funding, insurance coverage for abortion, and protections for patients and clinic staff. States were then assigned to one of seven categories based on the policies currently in effect and the cumulative impact of those policies on abortion rights and access"* [40]

[3]We used a locally run open-source transcription tool to ensure maximum data security and privacy, and that transcripts were not retained or used for any other purposes.

various points during the coding process, the first author met with the second and last author to discuss emerging themes. After coding all interviews, the first author arranged these codes into broader themes and met with the second and last author to refine and determine relationships between themes animating this paper.

We mapped the actors identified through our analysis using Bronfenbrenner's ecological systems theory [12]. EST offers a way to organize actors across different environments people may encounter or be influenced by, including the exosystem, microsystem, and macrosystem [12]. While we did not deductively code our data by applying EST, our analysis of actors mapped to the EST dimensions when organizing actors by their relationships with PCOPs.

3.5 Ethics

As researchers engaging with participants on topics of reproductive health, privacy, and technology, we recognize the great responsibility inherent in engaging individuals about these topics. We took several steps to ensure the privacy and safety of participants. It was important that data shared by participants could not be traced back to them in any way by any actors.

To ensure this, during recruitment and data collection, we took extra care to not encounter or collect any personally identifying information. This meant that we avoided any communication outside of the recruitment platform, prevented the use of personal emails, used ID numbers instead of names in all forms of communication and data labeling, and only interacted with participants through the recruiting platform to coordinate interviews and via a voice-only call for the interviews. The recruitment platform directly paid participants. At any point, we did not have access to any personal information to facilitate payment. Further, to protect participants' privacy, we used a locally run open-source transcription tool where no data were retained, stored, or used for any other purposes. After transcription was complete and manually redacted, all interview recordings were permanently deleted.

3.6 Limitations

We designed interview questions to be broad and as neutral as possible, inviting a range of perspectives to surface. However, our sample may be limited in the perspectives it covers: both people with extreme anti-abortion views or those with privacy concerns to the extent they feel unsafe talking about their reproductive health may have chosen to not participate. We used a recruiting service to engage participants, restricting our sample to individuals interested in research participation. Future work should seek to recruit a more diverse participant group along gender, race, and class dimensions. Additionally, our study presents a snapshot of how PCOPs were thinking about their reproductive privacy concerns and mitigation strategies, often speculating on what they *would* do or are currently worried about in a Post-Roe U.S.do or are currently worried about in a Post-Roe U.S. However, approaching this study's research questions with other methods, such as through diary studies or longitudinal survey approaches, would provide us with a better understanding of how people's reproductive privacy concerns and technological strategies change across time and space. This would be particularly helpful given the rapid changes in the U.S. political landscape for reproductive rights and the importance of understanding the toll of laboring towards reproductive privacy in a volatile climate for PCOPs. This would also be challenging to accomplish ethically, due to the increasing risks associated with reproductive health data in the US.

3.7 Researcher Positionality Statement

We are HCI and social computing scholars whose value systems of bodily autonomy, privacy, and reproductive justice shape this work. Our commitment to these values shaped our engagement with participants and contextualization of their experiences. We view the overturning of Roe v. Wade

as part of a larger historic threat to reproductive justice in the U.S. Accordingly, we contextualize our study and its findings within the larger history of reproductive (in)justice and infringements on reproductive rights in the U.S. *(Section 2.2)*. While Roe v. Wade was a critical foundation for reproductive rights, we recognize it as one piece of a much broader framework, and not the ultimate safeguard. This broader framework accounts for other reproductive health experiences such as those involving miscarriages, assisted reproductive technology, pregnancy, and contraception. We, however, did not indicate these views to respondents unless it came up in the conversation and it felt necessary to establish trust.

4 FINDINGS

We begin by detailing participants' reproductive privacy concerns and perceived privacy risks (RQ1). We then report on the technology strategies participants reported employing to help mitigate their reproductive privacy concerns (RQ2).

4.1 Reproductive Privacy Concerns in the Sociotechnical Post-Roe Context

Many actors—human (e.g., family, governments) and not human (e.g., legislation, algorithms) shaped participants' reproductive privacy concerns. We situate participants' perceived concerns and relevant actors using Bronfenbrenner's ecological systems theory (EST) [12]. EST provides a framework for organizing the many different environments an individual interacts with and is influenced by such as the microsystem, ecosystem, and macrosystem [12]. Microsystem refers to pieces in an individual's immediate environment that they're able to come in direct contact with and influence bi-directionally [12]. Exosystem, on the other hand, refers to specific formal and informal structures that can shape how a person experiences their microsystem and day-to-day [12]. And lastly, Macrosystem describes the intangible social, cultural, and political elements (e.g., beliefs, norms) in society within which an individual exists [12].

While we did not set out to use the EST, we find that our analysis of actors mapped to the EST dimensions. Within their **microsystem**, participants described privacy concerns involving their immediate, closest environments: family, friends, (ex-)partners, co-workers, employers, and healthcare providers. Among their **exosystem**, participants explained privacy concerns involving informal and formal structures: insurance companies, religious institutions (e.g., churches), local communities, anti-abortion organizations, authoritative bodies like the government and law enforcement, general "hackers and scammers", and Big Tech and its various elements (e.g., social media, search engines, data brokers, algorithms/AI). And, among the broader **macrosystem**, participants identified cultural and social norms that posed risks to their reproductive privacy: conservatism, the stigma surrounding reproductive health, and the politicization of accessing certain types of reproductive healthcare.

Participants thought of reproductive health as a uniquely privacy-sensitive context due to its heavy politicization in the U.S. and its intimate nature. As Yasmine explained, *"Reproductive health is a very personal, loaded topic for me, both politically, personally, otherwise."* This perception caused some participants, like Roxana, to argue their privacy concerns were *"more specific to reproductive [health]"* than other types of health. All participants' perceived privacy risks and prosecutorial consequences relating to abortion and a range of reproductive healthcare and experiences (e.g. contraception, miscarriages, (in)fertility, menstrual cycles) existed before and after the overturn of Roe—even if recent changes in legislation heightened reproductive privacy concerns or made them more immediately relevant for some.

Participants' reproductive privacy concerns emerged from uncertainty and a sense of having little control over the information flow of their reproductive health information (4.1.1). Concerns about having less control often related to legal consequences from governing bodies and an awareness

of the sociotechnical risks to reproductive privacy that emerged from their online data (4.1.2). One salient aspect of these sociotechnical risks was the inability to prevent others (e.g., big tech, governments) from making inferences about one's reproductive health status based on their data (4.1.3). Participants' understanding of reproductive privacy threats increased the burden associated with reproductive healthcare (4.1.4). Lastly, participants expressed general well-being concerns as a result of mismatches between their own social and cultural beliefs, and the social and cultural norms of those who had some form of power over their lives (4.1.5). Throughout, the breadth of privacy risks participants identified reveal how intertwined their reproductive privacy concerns are with actors at the micro-, exo-, and macrosystem [12] levels and how intricate and complex the undertaking of protecting one's reproductive privacy is post-Roe.

4.1.1 Loss of Control: Realizations about Uncertain Information Flows. Many participants indicated they have always been somewhat worried about control over their reproductive health information (e.g., medical records, texts, photos, search data) but feel that changes to legislation have made the risks more vivid and added to their uncertainty about where their information flows (e.g., doctors office, big tech, governments). Participants described several scenarios in which information about their reproductive health might be disclosed to an unwanted or unpermitted person(s) or other actors (e.g., algorithmic systems, tech companies, and law enforcement). Yet they also expressed many unknowns, for example, where their reproductive health information sits and who has access to it (e.g., family, information technicians managing electronic health records, doctors).

Alya *(woman, protective state)* described concerns that information shared with her doctor may not stay within the confines of the appointment and spread to others within her microsystem, such as her family:

> *"the only concern I would have is making sure ...what we speak about kind of stays within that room. Like, it doesn't leave, like, the clinic or office setting...So if it was something I didn't want my, I guess, my family to find out about...I would want to make sure that the conversation stays within that visit."*

Alya, like other participants we spoke with, was uncertain of who had access to her medical data and how it flowed.

Beyond the uncertainty of who can access their reproductive health data, participants also expressed concerns with the *type* of data that may be accessed and *how* it might flow from them to individuals or groups that may then act on it (e.g. governments, family). Participants expressed reproductive privacy concerns involving their medical records and digital footprints, including information shared with or accessed by others without their consent due to legislation or the government permitting or demanding access. These concerns implicate ever-changing laws that govern reproductive privacy, such as who has access to their data otherwise protected under HIPAA [1][4]. Valerie *(woman, most restrictive state)* feels certain she can trust her doctors to protect her information rooted in ethical professional guidelines but also worries that legislation could get in the way of these rights, even preventing her from obtaining birth control.

> *"I am a little bit nervous about my privacy and I trust my doctors but if they make laws that override the—what's the...the "hippocratic oath" or whatever, that would be bad...I mean, they're already forcing us to not be able to get abortions. But they could, they could criminalize being on birth control at all."*

[4]The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established standards and regulations aimed to protect the privacy of individuals' personal health information (PHI) and medical records [1]. In 2024, the Office for Civil Rights in the Department of Health and Human Services issued a reproductive-health specific rule to protect the privacy of individuals' health information pertaining to lawful reproductive healthcare under certain circumstances [87]

In this way, Valerie's concerns about her privacy are also heightened by fears of escalations in the law and how this may impact reproductive information flow.

Aliza *(woman, protective state)* described a similar concern with uncertainty over corporations reliably protecting her reproductive privacy in light of governments possibly forcing them to release information about users of technologies like social media or period tracking apps:

> *"I do think that if the government were to be like, 'we need all this information' that we all thought were private, 'we need to go through it right now for legal reasons.' I feel like they would just give it to them without much of a fight. I don't have a lot of faith in different companies going to great lengths to protect the people who use their product."*

Aliza is concerned about companies' willingness and ability to protect their consumers' information when authorities demand access (i.e., for legal prosecution), introducing uncertainty into how her reproductive health information might flow.

Both Valerie and Aliza's concerns regarding uncertainty over who can access their reproductive health-related medical records or associated digital footprint are the result of the ever-changing landscape of legislation governing reproductive privacy *and* the possibility for government overreach into an intimate part of their lives including in collaboration with technology companies.

4.1.2 Worries and Extrapolations of Targeted Legal Harm(s) Imposed by Governing Bodies. While these concerns about losing control often related to legal consequences, most participants we spoke with were not all that worried about an unintended pregnancy. Rather they speculated about prosecutorial harms that could befall them *if the unexpected happened* (i.e., they had an unintended pregnancy), or if they were to help others with an abortion, or the laws became more stringent (e.g., if laws were passed criminalizing birth control or gender affirming care). These threats were, for some, very vivid, either because they felt more at risk (e.g., because of their stage of life or location) or because they were able to think through the consequences of emerging laws and political trends. Participants had a good sense of the ways they might lack control of their reproductive health data and the legal implications. While they tended to think about their risks (or those of others) in varied ways (e.g., based on identity characteristics, social capital access, and health status), their understanding of sociotechnical risk often coalesced around fear of inferences based on their online data (e.g., dragnet warrants to gain access to shopping habits that revealed pregnancy), and less often, local threats initiated by others like unwitting physicians.

Participants were concerned that their information (e.g., medical records, online behavior, app usage, photos, texts, and emails) might be accessed by the government via unwanted surveillance. Participants frequently referenced state governments and Big Tech companies (e.g., Meta, Google) as being part of a relationship where the average user of a technology and their data is part of a dragnet[5]. Valerie *(woman, most restrictive state)* expressed concerns that photos stored on her phone—which included a photo of a possible miscarriage—could be accessed and monitored by the government or law enforcement to detect evidence of a supposed crime (i.e., an illegal abortion):

> *"It could get to the point with technology and politics and everything where they have access to, like, the pictures that you have saved and, like, Google photos or whatever and they can say, 'oh that looks like a miscarriage, better make sure she didn't cause that herself'".*

Many participants were concerned about the possibility of new laws that would allow authorities to gain access to intimate data stored on personal devices (e.g., mobile phones) due to the escalation of policing certain reproductive health experiences across the U.S.

[5]A dragnet refers to a type of surveillance where there is "the collection and analysis of information on everyone, rather than merely those under suspicion," across space and time [11]

Shauna *(woman, restrictive state)* speculated further on concerns of the reproductive health-related behaviors of people capable of pregnancy being monitored by their state's Attorney General whom, they speculated, might access their Amazon or pharmacy records in a kind of surveillance dragnet of anyone who had purchased medication to prevent pregnancy (e.g., Plan B[6]) or even just stopped buying period-related products:

> *"Is the Attorney General going to say we need to get all of the Amazon's sales for Plan B or, you know, Walgreens information or CVS or, you know, how many women are between this age group, how many women are buying feminine napkins so we can kind of narrow down and say we have so many women in [STATE] who potentially could be, you know, in this stage of reproductive health...?"*

Similarly, Noor *(transgender man, most restrictive state)* described concerns about law enforcement prosecuting her for certain reproductive health experiences: *"[concern about] local law enforcement...in case I ever did, uh, have an abortion or they thought I had...even if it was just a miscarriage or something, and then I was facing legal troubles for it."*. Aliza *(woman, protective state)* also shared concerns related to legal consequences and prosecution for helping others access an abortion when it violated her state's laws: *"[concerns of] like getting arrested, haul[ing] me away and like throw[ing] me in prison."* All in all, participants shared concerns that information regarding their personal and assistive involvement in accessing reproductive healthcare could lead to targeted harm by governing bodies.

Many participants envisioned several types of sensitive information produced as a result of their technology usage that might be incriminating, mainly involving the types of information and content visible in their digital footprint. In the aftermath of Roe v. Wade, Roxana *(woman, most restrictive state)* learned that using technologies like period tracking apps could produce data that could be used to connect her with criminalized reproductive health experiences (e.g., abortion):

> *"I did have a period tracker, but I read something about how...that information can be used and it can be gathered and then used to find out, like, for abortion...I feel like I'm stretching here or like reaching here. But I remember reading this a while ago...when Roe v. Wade was messed with and states were not allowing abortions and [Planned Parenthood said] get rid of any kind of tracker because they're gonna, you know, they're monitoring...whoever they are. They're monitoring, you know, this information."*

Roxana's awareness of how data from her period tracking app might be used against her occurred during a time when popular media (misleadingly) positioned period tracking apps as *the primary* threat to one's reproductive privacy [57]. Through consuming this media in the wake of the overturning of *Roe v. Wade* and changes to her state's legislation, Roxana is an exemplar of participants growing concerned about how their digital footprints might be incriminating if they ever need an abortion.

Notably, participants with multiple marginalized identities (e.g., race, gender, disability, class) frequently described their concerns for legal harms as interconnected to larger patterns of intersectional [23] vulnerability. For example, Kai *(transgender man, protective state)* described concerns about being impacted by the increased policing of trans and reproductive health care:

> *"I'm concerned that with the way things are going in the government any private information about someone being trans or seeking reproductive healthcare...could potentially be turned over to the government in the future to either increase surveillance on someone or ultimately, you know, issue criminal charges or things like that."*

[6]Plan B is a "morning-after emergency contraception pill" that can reduce the chance of pregnancy if taken at least 3 days after unprotected sex [68].

Kai is concerned that reproductive care could be surveilled and criminalized, mirroring threats to another dimension of heavily politicized healthcare (e.g., gender affirming care for Trans people) [50, 51]. While participants in our study had many shared reproductive privacy concerns, those who identified as belonging to groups subject to heightened policing framed these concerns within a broader network of threats. They emphasized how these threats could extend to the regulation of other intimate aspects of their own and others' embodied experiences.

Participants' fears of their reproductive health information becoming a threat were informed by their belief that they might unknowingly reveal information about their reproductive health through their technology usage.

4.1.3 Inability to Avoid Inferences Made by Powerful Actors Based on Reproductive Health Data. Participants expressed concern that their tech usage might reveal information about themselves that could be pieced together to make inferences about their reproductive activities, with or without their knowledge and certainly without their consent, that has prosecutorial consequences. But some, like Susanna *(woman, protective state)*, were also concerned with how these data could be used to learn things about her reproductive health related status, violating her privacy:

> *"With menopause or any other health issue that comes up, if there is...you search for it and the next thing you know,...the feed is populated with information about that and all. It's almost like you feel like somebody is watching and now, you know, somebody knows that...this is an area of interest and maybe that's what is going on in your life."*

Based on her behavior online, Susanna believes corporations using algorithms and others who may gain access to that information might be able to make inferences about her reproductive health. In this way, participants believed inferences about reproductive health based on one's digital footprint act as a threat (i.e., they may be assumed to have had an abortion and investigated) or as an uncomfortable privacy violation exposed through ads (e.g., when algorithms assume you are menopausal). Participants recognized their technological behavior produced information that can be used by governments and Big Tech companies to justify intruding on their reproductive privacy for legal or monetary reasons.

4.1.4 Increasing the Burden: Threats to Privacy Shaping Experience of Reproductive Healthcare. Participants' reproductive privacy concerns shaped how they experienced reproductive healthcare, imposing new burden [7] on decisions about whether to seek care and what to share, leading to a sense that they must be prepared for reproductive healthcare restrictions in the future.

For instance, Aliza *(woman, protective state)* described how her decisions about birth control were complicated in response to the reversal of *Roe v. Wade*. She worried that if she purchased birth control online, the government would find out, but that if she asked her doctor, they would think it was to avoid pregnancy. She ultimately decided to ask her doctor for birth control to treat her Polycystic Ovary Syndrome (PCOS):

> *"I first thought about using one of those apps where...you put in your information and then they send you the birth control by mail. But I was like, no, I can't do that. I don't want anyone to know...I just didn't trust them to not leak that information somehow to the government anywhere. But I trusted my doctor more, so I asked them to give me a prescription. But I did tell the doctor it was mostly for my PCOS...I was like, 'It's for PCOS to control like my periods and all that stuff.' And they were like, 'Sure.' And they wrote me a prescription, but I didn't tell them it was like specifically to not get pregnant."*

[7]We recognize as researchers that reproductive health is a context already riddled with difficult experiences (e.g., loss of life, mental health, maternal and infant mortality) that can be a burden in and of themselves. Here, we focus on the burden of trying to maintain one's reproductive privacy.

While Aliza wanted to go on birth control to not get pregnant after *Roe v. Wade* was overturned, the way she chose to access it was complicated by concerns that information collected by apps might be accessed by the government. Furthermore, despite trusting her OBGYN, Aliza's privacy uncertainty caused her to refrain from openly sharing why she wanted birth control.

Participants' worries about encountering legal harm prompted them to invest more time and resources towards managing their reproductive health and *defending* their ability to access reproductive healthcare in light of the unexpected. Some participants described speaking proactively with their doctors, partners, or friends to establish contingency plans in case their reproductive healthcare needs were no longer viable due to changes in their state's legislation. Serena *(woman, most restrictive state)* described talking with her partner about what to do if they needed an abortion, which is illegal in her state:

> *"We've kind of talked about like, you know, if we did need to receive access to medical care that was not available to us in [State], like an abortion or something else that was illegal in [State]....Like we do have family and friends that went outside of the state that we could visit...We had talked about what we could do if we did need something like that."*

The change of legislation in Serena's state caused her and her partner to dedicate time to develop a contingency plan if their reproductive healthcare needs were inaccessible where they lived. Similarly, Morgan *(woman, most restrictive state)* described how she made appointments with her healthcare providers to better understand what would happen in different scenarios given the restrictions in her state: *"I talked to my primary care physician. I talked to my OB-GYN. I actually made an extra appointment to go in and speak with them directly...I talked to my doctor, making sure I asked her specifically about what would happen..."*. Morgan and Serena, like other participants, allocated time, conversation, and labor to brainstorm future possibilities in light of uncertainty and a felt need to anticipate privacy threats that would limit their ability to access abortions and other desired reproductive healthcare.

4.1.5 Contentious Power and Mismatched Beliefs. While participants' reproductive privacy concerns were heightened in the Post-Roe context, they shared perpetual concerns for their well-being if their reproductive health information was discovered by actors in their microsystem (e.g. conservative family, manipulative parents) who they feared had the power to enact social, emotional and financial consequences, as well as actors in the macrosystem (e.g., state governments) who they believed had the power (de jure or de facto) to force unwanted physical experiences (e.g., forced birth). Participants' fear of those with power was shaped by their role in the relationship (e.g., as a child, as a resident of a particular state) as well as the social and cultural beliefs of these actors (e.g., being politically conservative, being 'pro-life', shaming premarital sexual relations). These fears increased anxiety for how participants' well-being would be adversely impacted if their reproductive health experiences clashed with the social and cultural beliefs of those who they felt had power over their well-being.

Yasmine *(woman, protective state)* feared a mix of emotional and financial consequences if her conservative family ever learned she was pregnant or might have a sexually transmitted disease (STD), especially due to her relationship status (i.e., single) causing her engagement in any sexual behaviors to contradict what her parents deemed appropriate:

> *"...Because I'm single, unpartnered, unmarried, if my parents were to find out that I was pregnant, then that would be very uncomfortable. If this happened like nine years earlier, then it would be dangerous and...I'd probably get taken out of college, I'd probably lose access to financial support...I would very much worry about my financial stability and my financial safety and emotional safety...If they found out that I was pregnant and had*

> *a miscarriage, they'd probably [judge]...For STD tests, I think they would judge me more harshly...I think I would lose...familial emotional support...Before it was like a financial issue and an emotional issue, and now it's just purely an emotional issue and just fear of judgment..."*

Yasmine's concerns of how her parents might wield their power changed with age (from more financial to emotional), due to changes in who had power over what as Yasmine got older. Other participants shared how their reproductive privacy concerns stemmed from a sense of paranoia and the realization that their reproductive health information could be used by those in their lives to manipulate them (e.g., reproductive health, career, relationships), leading to emotional harm. Morgan *(woman, most restrictive state)* was afraid her mother could use information about her reproductive health (e.g. if she were to have an abortion) as a way to control her or to ostracize her from other relationships (e.g., family, friends):

> *"...If [my mom] were to find out things, it's not safe for her to know about my health...my fear is that she would try to use it against me...My mom, if she were to get a hold of information, if I had an abortion or [other] certain reproductive health choices that I make, she could use it to try to alienate the family from me or to try to talk to my friends."*

Morgan notes that others she did not trust knowing about her reproductive health experiences makes her vulnerable to manipulation, ostracism, and control if they were to act in their own power based on their social and cultural beliefs concerning reproductive health. Cheyenne's *(woman, protective state)* concerns extended beyond individuals she knew, but rather strangers emboldened by their anti-abortion stance to take information about those who've had abortions to commit targeted physical harm against those who've received abortions:

> *"I think abortion tends to be extremely controversial and it's to the point where people can get violent about it. So, I'd be really like worried if people could have access to a database of people, their names and their addresses, and who has had an abortion. I think there could be someone really radical who would physically want to hurt people who have had abortions, and then I would be at risk. And then that would put my safety at risk…that would be…the most extreme situation where I'd be extremely concerned about my information getting leaked. All of the other stuff, like if I've had a pelvic exam or not, that's kind of like, okay…I don't think it would jeopardize my safety at least. But this is kind of, I feel, a very serious piece of information that could put my life in danger and that would make me really concerned. I probably wouldn't even want it documented that I've had an abortion."*

Cheyenne reflects an understanding of how beliefs around certain types of reproductive healthcare (e.g., abortions) can inspire fear of experiencing physical harm, while also noting how the *content* of any leaked reproductive health information (e.g., pelvic exams) can shape the level of degree for this concern. In other words, while participants feared the consequences of their reproductive health information flowing to nefarious actors who had power over their well-being, the type of reproductive health experiences they had that could then be reflected in their data mattered for how concerned they'd be about information being leaked.

Beyond others like family and friends, participants' reproductive privacy concerns stemmed from fear that those with the power to pass legislation criminalizing reproductive healthcare might produce realities where they would experience physical well-being harms—such as being forced to give birth. When explaining why she did not want the government to have any reproductive health data (e.g., ovulation data), Simone *(woman, protective state)* mentioned hoping to avoid a scenario where a government could determine a person's pregnancy outcomes (e.g., when they get pregnant, if they choose to keep or terminate a pregnancy):

> *"I just feel like if [the government] knows that information, [when I ovulate], they could potentially use it in a nefarious way…I feel like the government wants to control when you get pregnant. They want you…to have the baby. They don't want you to have a choice whether or not to keep the baby…I feel like [the overturning of Roe] was the federal government's way of saying we don't care about reproductive rights."*

Simone was cognizant of the possibility for information about her reproductive health to be misused by the government which she believed had the power to force unwanted bodily experiences on her, leading to physical and other harms.

Now that we have described participants' reproductive privacy concerns, we turn to discuss the strategies participants described implementing in response to these concerns.

4.2 Technology Strategies to Mitigate Reproductive Privacy Concerns

Most participants made connections between their reproductive privacy concerns and the ways they use technology. But when it comes to managing perceived risks, reactions ranged from little to no changes in how they used technology to high levels of intricate changes.

Technology Strategy	Technology Referenced
No Change	Devices Location, Devices Used, Information Disclosure, Online Search, Online Shopping, Online Support Groups, Social Media, Text/Email, Tracking App(s), Web Browser(s), Websites Visited
Abstaining from a Technology	Devices Location, Devices Used, Menstrual and Fertility Tracking Apps, Online Support Groups, Tracking Apps (Other)
Deliberately Modifying or Aiming to Erase Reproductive Health-related Digital Footprint	Browsing History, Devices Used, Devices Location, Information Disclosure, Mobile Devices, Online Search, Password management, Private Messaging, Social Media, Text/Email, Tracking Apps (Other), Web Browser, Websites Visited
Prioritizing Privacy Affordances (Explicit and Signaled)	Devices Used, Information Disclosure, Online Search, Online Shopping, Password Management, Text/Email, Voicemail, VPNs, Web Browser(s)

Table 2. This table described the types of technological strategies participants described making to mitigate their reproductive privacy concerns. For each strategy, we've listed the types of technology or behavior mentioned.

4.2.1 No Change. While participants detailed many different reproductive privacy concerns (4.1), these concerns did not always directly translate to mitigation strategies with technology, for reasons having to do with some combination of convenience, ability, awareness, and perceived risk. Darcy *(woman, restrictive state)* prioritized convenience when selecting devices: *"I just use whatever is most convenient to me."* A few participants speculated that while they currently have not changed their behaviors with some technologies, that could change depending on their reproductive health

needs or changes in legislation. For instance, Julie *(woman, restrictive state)* considers a range of digital traces from shopping to texting that could incriminate her if abortion became illegal in her state but since she lives in a state currently without restrictions, she has not changed her behavior.

> *"There's a famous story about Target sending a girl some 'welcome your new baby kit' or whatever to her parents' house because they could tell from her shopping habits that she was pregnant and her family didn't know because she was a teenager. I know that that is a thing. And I know from my days of smoking marijuana that you don't wanna text about illegal things, right? But I am not actively in a place where those are front of mind. I think if they were front of mind for me, I absolutely...like if abortion was illegal in [State], I would not text about an abortion, right? I would say I would have that conversation in person. I have an Alexa and sometimes she just like lights up yellow, right?...I would hopefully think about those things. I am not currently texting about abortion and I also live in a state where now it's legal."*

Julie's perspective illustrates how participants' decision to change their technology behaviors is partly dependent on their perception of reproductive privacy risk related to legislation in their state.

4.2.2 Abstaining from Technology. Some participants' reproductive privacy concerns motivated them to abstain from certain technologies—like menstrual and fertility tracking apps, online spaces like Reddit, and public computers (e.g., at the library) or public Wi-Fi. Morgan's *(woman, most restrictive state)* desire to maintain reproductive privacy prevented her from using public Wi-Fi when researching about reproductive health: *"I no longer use public access Wi-Fi at all...when I do work with health-related stuff, when I'm doing research or whatever."* Likewise, Kai *(transgender man, most restrictive state)* described that he had stopped using menstrual tracking apps following the overturning of *Roe v. Wade* due to inferences that could be made about his reproductive health (because he has the app on his phone) or possibilities for his reproductive health data to be accessible to Big Tech:

> *"I completely stopped using [period tracking apps]. I used to use them a little bit. But I don't honestly feel comfortable using them anymore, especially because a lot of them require you to sign up with Google or with Facebook or something like that. And I'm just like,...I don't want it displayed on my Google account or whatever...just simply having that app installed reveals a lot about me...So I'm very cautious about that...it was after Roe v. Wade was overturned. I feel like that was something that just made me like, 'wow, I do not want to have any of my reproductive health information available to these giant tech companies'."*

Kai believes that simply by having a period tracking app on his phone, his reproductive health information is endangered.

As another example, Aliza *(woman, protective state)* explained that she had stopped participating in an online support forum on Reddit designed to connect people seeking an abortion or other contested reproductive health care with others out of fear of being doxxed or the government finding out, even if she didn't think what she was doing was illegal per se:

> *"On Reddit, I was a part of this, it's called [name redacted], and it's for people who live in states where abortion is illegal, and they need to travel to a state where abortion is allowed. And I live in one where you can get an abortion. And...they help you with like traveling and giving you a place to stay. I was part of that. And then I kind of like stopped just because I was like worried I would get in trouble somehow....I was worried that somebody would dox me and find out and somehow I would get in trouble. I don't think it was illegal what I*

> *was doing, but I was still worried...I'm just so paranoid that somehow all this information will get leaked to the government and they will crack down on me somehow, even though I don't think I'm doing anything wrong."*

This example foregrounds how people's reproductive privacy concerns may have consequences for the maintenance of social support networks for sensitive reproductive contexts Post-Roe. Likewise, participants' experiences highlight how reproductive privacy concerns may lead people to refrain from using technologies they otherwise would use. In this way, the factors that produce these privacy concerns concerning reproductive health may act as barriers to choice.

4.2.3 Deliberately Modifying or Aiming to Erase Reproductive Health-related Digital Footprints. Participants shared changes they had made to significantly reduce or delete their reproductive health-related digital footprint. These included not sharing or engaging with anything about reproductive health on social media, refraining from texting/private messaging/emailing about reproductive health, avoiding visiting websites related to abortion or searching online about abortion, being more selective when searching about their reproductive health online, and not seeking reproductive health information on shared devices.

Aliza *(woman, protective state)* said she stopped texting her friends about aspects of her reproductive health, like when her period started, because she worried about it "sitting on a server" somewhere and it being hacked or simply requested by the government and used against her as evidence:

> *"I didn't want...to have it written down somewhere, like sitting on a server that could be the information taken and used against me. And I'm realizing now...how paranoid I am about like people knowing when I have my period...Through hacking or like, I don't know, the government contacting Google and being like, we need all the records, like we need to go through them."*

For those who continued to communicate about reproductive health online, they chose to use vague language. Noor *(transgender man, most restrictive state)* explained how his concerns that an online platform, like Discord, may share his messages with others (e.g., governments) prompted him to be more circumspect:

> *"When I'm talking to my friends over Discord and stuff, I do try to be careful with what I say because it's not like Discord's not gonna give messages to whoever if they need to..so um I do try to to be cautious with what I'm saying,...not saying anything...specific, like I'll be like, 'Hey, this is a resource that you could possibly use' and not like getting into conversations about if someone does specifically use that [or] go through that resource or not. You know?"*

Noor uses nondescript language when sharing information about reproductive health online, in part because of a distrust in social platforms to protect the privacy of his conversations with friends if a government were to mandate this information be released.

In response to concerns that their reproductive health information and online content they engaged with could be surveilled and accessed by others (e.g., governments and big tech), participants chose to modify what types of data were stored on their devices. Kai's *(transgender man, most restrictive state)* reproductive privacy concerns led him to make changes in his mobile phone to reduce data storage and tracking: *"[My reproductive privacy concerns] made me more cautious about really looking into my settings on [my phone] and increasing my privacy and decreasing like tracking and information storage as much as I can on this device."* While changing settings on the back-end of devices was not commonly reported, it was clear that participants hoped to limit the amount of reproductive health information that could be traced back to them.

Some participants detailed how their reproductive privacy concerns prompted them to avoid certain technology and disclosures—for example, not using medication reminder apps for birth control, and limiting personal information (e.g., biological sex) when creating accounts online. Noor *(transgender man, most restrictive state)* described that he limits disclosing his biological sex when signing up for certain apps so that the possibility of someone making assumptions about his reproductive capacity is reduced:

> *"For things that don't have a good gender selection, for apps and stuff like that, in the past I never had a particular issue for choosing female if that would actually have some effect on it that might be useful...but now it's like nope, i would like to pick Male...For some stuff it might ask questions..like if it's a, you know, health type app, it might ask questions that are related to my period or whatever. And it's just like, I just do not want to even see that option now. Cause I do not want to fill out that information."*

Noor illustrates how privacy concerns for reproductive health might prompt some to constrain their behaviors in sociotechnical spaces online—in this case, limiting what information one discloses due to its possible connection to characteristics about oneself that may bring assumptions about sensitive bodily experiences and render oneself more vulnerable to reproductive privacy risks. In this specific instance, Noor disclosing his biological sex or assigned gender at birth might hint at other vulnerable characteristics (e.g. being trans, having a reproductive system capable of pregnancy).

Participants also obfuscated [13] their footprint by deliberately adding ambiguity as a way to assuage concerns of having potentially incriminating or vulnerable reproductive health information or experiences reflected in their online data. Participants mentioned investing extra time and effort to obscure their reproductive health-related digital footprint to have less incriminating data. This included behaviors like clicking multiple unrelated resources when making a sensitive online search, visiting multiple websites to 'clutter' one's browsing history, using vaguer language when searching about reproductive health online, and keeping information disclosed in sociotechnical spaces generic. For example, Noor *(transgender man, most restrictive state)* explained that when making an online search related to reproductive health, he will use vague language and deliberately click on multiple websites that are unrelated to the task at hand. A desire to seek out information about reproductive health while still being able to maintain some level of ambiguity or deniability in the case of legal consequences motivates Noor's online browsing behavior:

> *"I feel weird when searching certain things around reproductive health care now...So sometimes, even if I do need to search for something, I try to search for it with vaguer language. Then, look at multiple resources [where] some of them clearly don't have the information I'm looking for on a page. But yeah. The goal [is] if I'm using bigger language and looking at like multiple resources on a thing, it is less specifically like, 'oh, so that is what you were searching for', you know, in case, like there's ever any like legal stuff going on or whatever....So depending on what pops up when I search, I might just look at five or so things that pop up on the first page of the search, even if it's pretty clear from what you can see from the search page that it doesn't have what I was looking for...Just so it's not as directly traceable for what I was specifically searching."*

Similarly, Aliza *(woman, protective state)* would only click an article about abortion if it was in a major news source but would never seek it out through search, giving her plausible deniability should abortion become illegal in the U.S. (evoking Nazi Germany):

> *"If it's on the front page of the New York Times website or the front page of the CNN and they're talking about, you know, 'this state has now ruled out abortion'...I'll click on it, but I'm not gonna actually search it out, if that makes sense...If somehow abortion was illegal*

> *tomorrow in the U.S., and nobody's allowed to read about abortion or something...I'm thinking in Nazi Germany, where they made so much information illegal...I'm like, oh, I could argue that it was like, I like accidentally clicked on it when I was looking on CNN and I read it or something, but I didn't Google it and like actively search it out. So I didn't really do anything wrong. Like that would be my argument. Like I want to be able to be like, to like have an excuse."*

Both Noor and Aliza's attempts to conceal their reproductive health-related footprint are illustrative of the labor of managing reproductive privacy concerns in a social, political, and cultural context where reproductive health is increasingly politicized and surveilled.

Participants also detailed efforts to delete their digital footprint completely, but found it an almost herculean feat. Most commonly, they referenced efforts to delete data stored as a consequence of their technology usage (e.g., browsing history, clearing cache, automatic log-ins).

Morgan *(woman, most restrictive state)* explained how she manually deletes her search history and cache whenever she has been researching sensitive topics or shares a device with another person:

> *"Sometimes I delete specific search history...I clear out the cache after I've looked at certain websites regarding my health...I don't usually consider myself a conspiracy theorist but I get anxious if I am doing a lot of research and someone is going to be looking or using my device and seeing that search history in relation to that."*

As a result of anxiety over her reproductive privacy, Morgan tries to erase her digital footprint so that the websites she has visited and online search data are destroyed. Similarly, Kai *(transgender man, most restrictive state)* described configuring his web browser so that he limits how much data is automatically collected (e.g. automatic log-ins) and ensures his digital footprint is erased periodically:

> *"I have [my web browser] set to Delete all my history after a certain number of months...I also don't let Firefox save any of my logins or things like that. I try to keep as little information about me stored in the browser as possible...it's not so much directly connected to reproductive health but I feel like those feelings about reproductive health do kind of like play a role in my overall privacy concerns."*

While Morgan and Kai's efforts to erase their digital footprint weren't unique to reproductive health, they illustrate how one's reproductive privacy concerns can motivate action to manage the default persistence of online data. In other words, unless participants deliberately took action to delete their online data, their data—reproductive health related or not—would likely persist and exacerbate their sense of threat.

4.2.4 Prioritizing Privacy Affordances (Explicit and Signaled). Participants' reproductive privacy concerns shaped their decisions about which technologies to use based on their privacy affordances and reputation, such as by prioritizing devices or web browsers that offer more privacy controls. Kai *(transgender man, most restrictive state)* explained that he switched browsers due to one having more privacy settings than the other, *and* being more disconnected from Big Tech (e.g., Google): *"Within the past, like, two to three years I've started only using [web browser] Firefox instead of using Chrome or things like that because Firefox has more privacy protection than isn't connected to Google."* Others like Yasmine *(woman, protective state)* explained they used both web browsers Firefox and Google Chrome because they were familiar with and had trust in the settings used to protect their privacy and assuage their privacy concerns:

> *"Particularly with regard to searching reproductive health things, I think that both Firefox and Chrome would allow me to have...a reasonable amount of control over what aspects*

> *of my data or search history are shared or not recorded or anything like that...I have a better understanding of how to do things like delete cookies, delete cache, delete search history on those platforms versus other ones."*

While Kai and Yasmine have different perspectives on the level of privacy afforded to them on web browsers, it is clear that their choices for which browsers to use were informed by their perception of a browser's privacy affordances and their desires to maintain reproductive privacy.

When a technology's baseline affordances did not provide a sufficient sense of privacy, participants, by necessity, took the responsibility to manage their own reproductive privacy concerns. Some took it upon themselves to incorporate additional technology to meet their desired reproductive privacy needs. This included practices such as using a VPN, having separate accounts when being part of a shared online shopping account (e.g. Amazon Prime), taking advantage of a web browser's privacy or incognito mode(s), as well as incorporating a password manager to keep complex passwords organized. For example, Kai *(transgender man, most restrictive state)* explained how his reproductive privacy concerns were one of the things that contributed to his decision to use a VPN when seeking out sensitive information online (e.g., reproductive health, trans health): *"I feel like over the past, like, year or two, I've gotten I've just gotten more cautious about using things like VPNs, especially when I'm browsing for sensitive information."* Similarly, Yasmine *(woman, protective state)* described using a private browsing mode when searching for information about ectopic pregnancy symptoms despite not sharing her devices with others:

> *"So even though no one has access to my internet history because I pay for my own internet, no one looks at my phone or anything like that, I still went into private Google search and or like whatever, the incognito mode. And then I double checked that none of my search items popped up when I like switched back.... I was very mindful of the fact that I should reduce my digital footprint...".*

Even though Yasmine believes the chances of others viewing her browsing history are slim, she still navigates online searches in ways that minimize how much data is stored in her web browser.

Participants also described changing their communication modes based on perceived privacy affordances. Some participants described making changes to their communication permissions and behaviors concerning their doctors and healthcare providers, such as by not allowing doctors to leave voicemails on a phone or choosing to only communicate with their doctor via a patient portal. For example, due to wanting full control over who has access to her reproductive health information, Yasmine *(woman, protective state)* chose to alter how her doctor could communicate her health information with her, desiring ways that felt more secure to her (e.g., opting out of voicemails):

> *"I choose to not have my providers leave messages on my voicemail because I feel like I have less control ...If there's an option, I say, do not contact me via phone and do not leave voicemails with health information...It's unique to reproductive health."*

Importantly, when Yasmine has a *choice*, she chooses a form of communication between her and healthcare providers that feels more secure and aligns with her reproductive privacy desires.

Beyond communication with healthcare providers, other participants described altering their methods for texting or emailing, such as by using alternative messaging systems that use end-to-end encryption. Kai *(transgender man, most restrictive state)* perceives end-to-end encrypted messaging systems like Signal or email services like Proton Mail to be more secure than other forms of communication. In part, Kai's decision to use a tool like Proton Mail is due to its perceived protections against U.S. legislation like the Patriot Act that allows for governmental monitoring communications of U.S. citizens [3]:

> *"I use Signal for my text because it's encrypted. Very rarely only use my regular messaging app and I don't use gmail for any personal or health related communications....I'm usually doing things through Proton Mail and Signal...If I'm talking about anything related to being trans, anything related to healthcare, I'm definitely making sure it's being communicated in one of those more secure channels, or encrypted at least.... I feel a lot more secure using [Proton Mail's] services because they're headquartered in Switzerland so they're not subject to the U.S Patriot act or anything like that."*

Kai perceived a technology to offer more secure communication due to its privacy affordances (e.g., end-to-end encryption) as well as the legislation that governs the technology providers' infrastructure. In this way, companies based in locations with legislation that does not protect citizens' privacy, in some cases, actively allows governments to violate it are understood as offering less secure technology. Participants' experiences illustrate how people's reproductive privacy concerns might inform the usage of certain communication tools based on their perceived privacy affordances.

Overall, participants described a wide range of technological behavioral changes in response to their reproductive privacy concerns. These included no change at all or a complete abstention from using or engaging with certain technologies. It also involved efforts to deliberately modify or reduce one's reproductive health-related digital footprint and to prioritize technology with (perceived) privacy affordances.

5 DISCUSSION

We argue PCOPs are part of a *privacy vulnerable population*, which McDonald and Forte define as a population "whose members are not only more likely to be susceptible to privacy violations, but whose safety and well-being are disproportionately affected by such violations" [58]. While these privacy violations of PCOPs are not new (see 2.2), the stakes Post-Roe and the increased policing of people with reproductive capacity have exacerbated this vulnerability [37]. In the following sections, we outline our theoretical contribution of *sociotechnical reproductive privacy*, within which we introduce the concept of *reproductive privacy labor*, as a type of safety work [48] and data work [66]. We discuss a need to grapple with the persistence of digital footprints regarding reproductive privacy, before turning to reflect on the limits of regulating sociotechnical threats to reproductive privacy in a volatile U.S. political landscape.

5.1 A Conceptual Framework of Sociotechnical Reproductive Privacy: Actors, Technology, and Identity

Our findings suggest a broad range of contexts for the reproductive privacy concerns of PCOPs and the technologies with which they engage Post-Roe to address their concerns while navigating shifting relationships between actors, technologies, and their many identities. The individuals we spoke with are confronting a range of sociotechnical threats, including investigations of their social media accounts and other third-party data initiated by hostile healthcare providers, as well as the risk of surveillance and scrutiny of their activities on personal devices—such as browsing, purchases, location data, and messages exchanged with friends and family. These threats are further exacerbated by personal health and identity characteristics that increase their susceptibility to harm and influence the sociotechnical strategies they adopt.

To make sense of these dynamic contexts, we contribute a conceptual framework we call *sociotechnical reproductive privacy*. We define **sociotechnical reproductive privacy** as privacy pertaining to data that may be deemed as relevant to, or as evidence of individuals' reproductive decisions and experiences that may be both threatened *and* protected by the relationships between actors—human

and not—technology, and identity. We argue these three dimensions converge in dynamic ways to shape sociotechnical reproductive privacy risks, as demonstrated by participants' articulation of shifting relationships between several actors, technologies, and identities in their reproductive privacy concerns.

By formalizing this concept of sociotechnical reproductive privacy, we can better identify and discuss contextual factors [57] that make reproductive privacy risks more or less salient for this privacy vulnerable population [58] within a sociotechnical landscape that enables unprecedented levels of surveillance and threat [21, 25] to the intimate spaces of people's reproductive lives. The sociotechnical reproductive privacy conceptual framework is thus particularly valuable in a space characterized by this complexity of threats emerging from social, geographic, legal, health, and technical dimensions. It encourages researchers to look beyond singular technical threats, such as those posed by period tracking apps, and beyond personal, context-specific dimensions of threat, such as demographics. Our primary goal in introducing the conceptual framework of sociotechnical reproductive privacy is to encourage scholars to adopt a holistic perspective on reproductive privacy. By calling for scholars interested in reproductive privacy to be responsive to the shifting relationships between actors, technologies, and identities, this framework supports future work that looks to intervene, rather than simply produce a set of design implications or solutions [6, 27]. We thus present it as a concept for future exploration and empirical testing. Here, we begin to untangle the relationships from our findings that emerged between PCOPs and the various actors, technologies, and identities salient to their experiences of sociotechnical reproductive privacy.

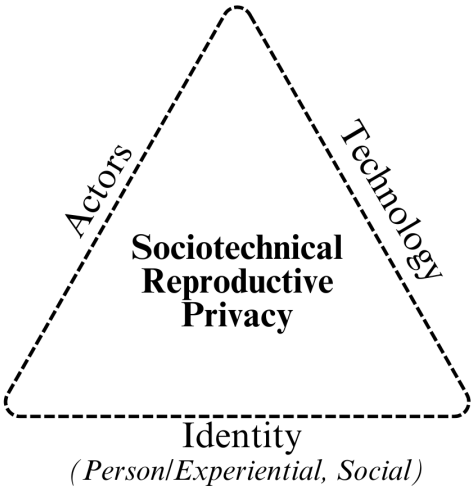

Fig. 1. This figure shows the three dimensions of *Sociotechnical Reproductive Privacy*: Actors, Technology, and Identity (person/experiential, social).

5.1.1 Actors. Participants identified a wide range of actors when discussing their reproductive privacy threats post-Roe. We detail these actors in Table 3, which span participants' immediate environments—such as work, home, and healthcare settings (microsystem)—as well as the (in)formal structures—such as health insurance companies, big tech, and local and state governments—they believe are surveilling them or have access to data they can act on (exosystem). Additionally, we consider the culture and norms surrounding PCOPs (macrosystem). These perceived relationships between a PCOP, and actors at the various micro-, exo-, and macrosystem levels were salient to participants' ideas around sociotechnical reproductive privacy risk., and the strategies individuals employ. For example, Yasmine's reproductive privacy concerns centered on the relationship between her parents (microsystem), data recorded on her health insurance statements (exosystem), and her family's conservative beliefs (macrosystem) around sexual activity or a possible pregnancy out of a marriage.

The range of actors understood as presenting various levels of risk in our conceptual framework paints a comprehensive picture of where perceived reproductive privacy risks and harms may stem from, offering a broad starting point for researchers, and reproductive rights and privacy

	Actors
Microsystem	Co-Workers, Employers, Family, Friends, Healthcare Providers, and (Ex-)Partners
Exosystem	Big Tech (e.g., companies, data brokers, algorithms/AI), Anti-Abortion Organizations, General 'Hackers and Scammers', Governing Bodies (e.g., State Government, Law Enforcement), Insurance Companies, Local Communities, and Religious Institutions (e.g., churches)
Macrosystem	Conservatism, Stigma Surrounding Reproductive Health, and the Politicization of Reproductive Healthcare

Table 3. Actors referenced in participants' sociotechnical reproductive privacy concerns, organized using Bronfenbrener's ecological systems theory (EST) [12].

advocates to tease out the nuances of their potential impacts. These perceptions of reproductive privacy risks not only shape what people may do to protect their privacy, but may also have downstream effects, for example, on their interpersonal relationships, access to critical care, and social support. For example, while abstaining from sociotechnical spaces like online support groups or refraining from communicating with people in their social networks about their reproductive health caused participants to believe they were protecting their privacy, it may also limit access to social support when and if needed. Additionally, sociotechnical reproductive privacy risks and concerns may actively impact individuals' abilities or willingness to try to seek out care or support. This is particularly important given how critical timing is for so many aspects of reproductive health (e.g., being turned away from receiving care after missing the window for accessing an abortion in your state [34]).

The level of granularity in this study is a departure from our existing knowledge about reproductive privacy in HCI that focuses narrowly on MFTAs [4, 26, 54, 59, 60, 62] or more generally on people's perception of privacy threats in the immediate aftermath of legislative change [57]. This study offers a novel level of granularity into privacy threats for PCOPs within a new sociotechnical chapter in the broader history of reproductive health and justice in the U.S. Rather than speculating on the possible risks or harms stemming from *each* of the possible and shifting relationship(s) between a PCOP and actor(s) identified by participants, the breadth of actors implicated in sociotechnical reproductive privacy should raise alarms for scholars, regulators, policymakers and technologists about how expansive the threats to reproductive privacy can be, perceived or experienced, for PCOPs. Future work could pick one or more of these actors as a starting point for teasing out more of the privacy risks or harms emerging from the relationship between actor(s) and other dimensions of sociotechnical reproductive privacy (i.e., technology and identity).

5.1.2 Technology. Participants mentioned many technologies when discussing their reproductive privacy threats post-Roe. These technologies, outlined earlier in Table 2, include things like geolocation, personal browsing, and social platforms, and correspond to any number of actors, such as family (who may surveil their activities), healthcare providers (with access to their records), and authorities (who surveil or investigate them). For example, Noor discussed privacy concerns and strategies involving messaging friends about reproductive health within the online messaging affordances offered by Discord. In describing his concerns and strategies, Noor accounted for possible entanglements between himself (and his data), his friends, the online platform, and the government who might be able to access and act upon Noor's digital footprint.

While prior reproductive privacy scholarship has largely focused on menstrual and fertility tracking apps (MFTA) (e.g., [16, 26]), our analysis provides a more comprehensive picture of the technologies that present (perhaps, greater) harm to participants and thus should be part of their strategies to mitigate their reproductive privacy concerns. Future research must grapple with these technologies and their many entanglements. Beyond the technological artifacts themselves, participants' reflections on technology's role in sociotechnical reproductive privacy also emphasized nuances around the characteristics of a technology's use and its propensity for risk, such as *when, where* and *how* a technology was experienced. Rather than delving further into the specifics of these technologies in this paper, we suggest that policymakers, researchers, and designers consider this range of technologies to promote sociotechnical reproductive privacy, and remain attentive to a technology's shifting relationship with privacy risk.

5.1.3 Identity. Participants referenced many overlapping and shifting identity facets when discussing the risk of encountering reproductive privacy harms post-Roe. Our findings show how PCOPs perceived diverse identity characteristics (e.g., marital status, gender) to converge to produce dynamic vectors of threat and risk to their sociotechnical reproductive privacy, outlined in Table 4. Identity may be conceived as *personal* (e.g., individual characteristics like marital status), *social* (e.g., membership in a certain group like race, class, gender) [14], as well as experiential (e.g., access to transportation, medical history). Beyond traditionally conceived social identity [14] facets where we might expect those with marginalized identities (e.g., race, gender, age, ability status) to experience increased harms from privacy violations [74], personal identity and experiential characteristics were also salient to participants' perception of sociotechnical reproductive privacy threat and the entanglements between technology and different actors in the micro-, exo-, and macrosystems. These included characteristics relating to one's reproductive health status, reproductive healthcare needs, reproductive healthcare assistance, surrounding environment/location, relationship to location, medical history, medications, and sexual or reproductive health behaviors. For example, Kai was a transgender man who lived in a protective state. His understanding of his risk for experiencing reproductive privacy harms was informed by his gender identity *and* the understanding that characteristics about his surrounding environment (e.g., legislation) were unstable and subject to change.

We align with prior work (e.g.,[14, 41, 75]) that we must think of identity in nuanced and expansive ways (e.g., social identity, individual or experiential identity such as medical predispositions or location) to allow us to contextualize the many types of characteristics shaping privacy threats across space and time. Rather than viewing identity as stable, latent, and essentialized, we learned from participants' experiences that identity is far more fluid and complex, entangled with other dimensions across space-time that shape instances of '(un)becoming' [39] vulnerable to sociotechnical reproductive privacy harms. Future research may further explore how these clusters of identities might shape experiences of sociotechnical reproductive privacy vulnerability. It could also explore how PCOPs use strategies to protect sociotechnical reproductive privacy, given the moving relationships between technology, different actors, and themselves. We do not make definitive assertions that all the identity characteristics presented in Table 4 are intrinsically related to how people experience technology or sociotechnical reproductive privacy risk. Rather, our contribution is in offering a detailed representation of how PCOPs consider identity as implicated in their vulnerability to sociotechnical reproductive privacy harms, and how these considerations shape their efforts to manage risk.

We acknowledge that tackling issues of reproductive privacy, technology, and harm is complex. This is partly due to the entanglements of actors, technology, and identity that our analysis shows may produce shifting relationships with reproductive privacy threats and harms. By identifying

Identity Shaping Sociotechnical Reproductive Privacy Threat	
Identity Cluster	Types of Characteristics
Social Identity	Ability Status, Age, Biological Sex, LGBTQ Identity, Gender Identity, Race, Socioeconomic Status
Reproductive Health Status	(In)Fertility, Miscarriage, Pregnancy, Hysterectomy, Menstrual Cycle, STDs, Test Results, Abortion
Reproductive Healthcare Needs	Reason for Medical Visits, Needing Restricted Reproductive Healthcare (e.g., abortion), Needing Reproductive Health-Related Information
Reproductive Healthcare Assistance	Assisting with accessing legal Reproductive Healthcare, Assisting with accessing criminalized Reproductive Healthcare, Engaging in Reproductive Health Advocacy
Surrounding Environment/Location	Religiosity, Surrounding Community's Values, Legislation in State of Residence
Relationship to Location	Ability to Travel Out of State, Location of Healthcare Provider
Medical History	Medical Records, Information Flagging 'Poor/Weak' Health, Medical Predispositions
Medications	Birth Control and Contraception Use, Prescriptions, Access to Birth Control
Sexual or Reproductive Health Behavior(s)	Being Sexually Active, Relationship Status, Sexual Activity

Table 4. This table details the type of characteristics participants referenced that were salient to their conceptions of sociotechnical reproductive privacy risk.

these dimensions through the conceptual framework of sociotechnical reproductive privacy, we provide conceptual vocabulary to help make sense of all the dimensions we argue scholars *should* be thinking about that move beyond singular technological artifacts, identities, or actors—instead focusing on the *relationships* between these dimensions.

5.2 Reproductive Privacy Labor

Participants' experiences highlighted how much they labored towards sociotechnical reproductive privacy in a Post-Roe U.S. We conceptualize this labor as *reproductive privacy labor* to describe 'the sociotechnical labor individuals perform to manage their reproductive privacy, which may or may not lead to successful privacy protection'. PCOPs' reproductive privacy labor is a type

of safety work [48] interested in trying to stop privacy intrusions from happening at all. This labor is an expression of *situated agency* [89]. Understanding this agency as situated [89] means recognizing that PCOPs' agency (e.g., technology mitigation strategies) is both free and restricted, both a response to a society that polices those capable of pregnancy [37] *and* an expression of PCOPs' desire to try and reduce the risk of reproductive privacy violations in turn. In other words, many of sociotechnical reproductive privacy's elements are both a site for vulnerability, as well as a site for agency. For example, technology acts as both a source of vulnerability (e.g., surveillance, incriminating online data), as well as a source for agency (e.g., technology strategies) to try and protect one's sociotechnical reproductive privacy. Reproductive privacy labor manifested in the experience of participants whose sociotechnical reproductive privacy concerns caused them to abstain from or reduce their engagement with certain platforms and technologies (e.g., social media, online support groups, public Wi-Fi) causing inconvenience. It also showed up for those who had to spend more time (e.g., manually track periods, and obfuscate online searches), and may have missed out on important information about their health.

Participants efforts laboring towards sociotechnical reproductive privacy might also be understood as a form of data work [66], where individuals are burdened with managing and curating their data, including in healthcare [67, 85]. In healthcare, data work has been shown to extend the labor asked of frontline workers [85], as well as the labor of patients who must increasingly manage their personal health information [67]. While PCOPs may at times exist in the role of 'patient', participants in our study performed reproductive privacy labor on information relating to their reproductive health across many different contexts beyond healthcare. We argue their reproductive privacy labor is a type of data work relating to resistance and mediation [53, 84] in reproductive health contexts. Lu et al. discusses the data work of teachers that resist the surveilling gazes of parents, and administrators who may threaten their autonomy [53]. Similarly, in our study, participants exemplified the way PCOPs engage in labor to obfuscate their reproductive health information from the surveilling gazes of actors, like governments and law enforcement, who might access and react to their data in ways threatening their reproductive autonomy [21], such as Noor's decision to use less precise language when seeking information about reproductive health online. Furthermore, participants highlighted PCOPs' efforts to control the mediation of their reproductive health data across the different contexts, actors, and technologies where their information might flow.

Prior work on the precarity of data work in power-laden contexts has found that those who are 'powerholders' in asymmetric power relationships often control the means of data production, interpretation, and contextualization [64]. Reproductive privacy labor and the data work it entails exists in a power-laden context where PCOPs navigate asymmetric power relations between themselves and other actors with the ability to influence their lives (e.g., governments, big tech). However, despite these power asymmetries, within which PCOPs' reproductive privacy labor is situated, PCOPs still resist, and labor to protect their sociotechnical reproductive privacy.

It is important to consider how different identity attributes contribute to disparate sociotechnical reproductive privacy risk and the labor to mitigate this risk. While threats to reproductive health and privacy have always been inequitable [37, 72, 74], and technology in and of itself remains inequitable [20, 45, 47, 65, 88], these inequities extend to reproductive privacy labor. Reproductive privacy labor has the potential to impact some more than others, such as those of a lower socioeconomic status who might rely more on public computers and public Wi-Fi [24] or those in need of social support that are more likely to need online support spaces like Reddit [5]. Expansively thinking of identity (e.g., social identity, medical predispositions, location) allows us to be attentive to differences in privacy threats where PCOPs are forced to navigate already inequitable sociotechnical and reproductive health terrains, facing disparate harms both as a result of their reproductive privacy

being violated *and* the effects of needing to navigate these privacy risks via reproductive privacy labor.

While privacy scholars have been concerned with the burden of privacy management on users for a long time [56, 73, 82], formalizing reproductive privacy labor is useful as it has become a central part of living as a PCOP in the 21st century, where the policing of motherhood and criminalization of pregnancy [37, 44] is omnipresent [8]. Just as Kelly positions safety work [48] as a form of invisibilized work [83] performed by women in their efforts to prevent harassment and violence in a patriarchal society, reproductive privacy labor is a form of safety work *and* data work mandated of PCOPs facing rampant privacy threats.

5.3 Legislation, Sociotechnical Reproductive Privacy, and the Persistence of Digital Footprints

Participants believed their digital footprints may expose them to legal risk. The ever-shifting legal landscape controlling reproductive rights in the U.S. was salient to their reproductive privacy concerns and the strategies they chose (not) to implement as it necessitated a level of political attentiveness and a more reactive orientation in turn. Within this volatile and aggressive surveillance landscape, there is little to stop authorities, technology companies, and data brokers from using digital traces to make inferences about people's reproductive health characteristics and viewpoints (e.g., likelihood of pregnancy, birth control prescriptions, pro-choice attitudes) in ways that could be used in criminal investigations. The persistence of this digital footprint even allows for retrospective use of these data, even from *pre-illegal* periods! [25]. Already, many of the laws designed to limit disclosure of certain health information (e.g., HIPAA) make exceptions for law enforcement (e.g., not just seeking warrants for medical records but seizing personal devices in investigations) *and* there is nothing to prevent law enforcement or anti-abortion organizations from purchasing copious amounts of sensitive data from data brokers to infer, correctly or not, reproductive health-related information about PCOPs [9] and target PCOPs in various ways. The precarity of sociotechnical reproductive privacy in a post-Roe U.S. pushes us to question the ethics of digital data collection and data permanence. Participants' reproductive privacy concerns were heavily predicated on their digital footprints housing information that might allude to their reproductive health status. We assert that reproductive health-related data collection and storage are not neutral in an increasingly precarious surveillance state where individuals' datafied reproductive health information can be recontextualized as evidence against them, particularly as reproductive health and privacy laws shift, changing the legality of individuals' reproductive health experiences.

We are hesitant to provide solutions to this problem or offer formal implications for design [6, 27] in this paper. Instead, we aim to illustrate how messy the landscape of sociotechnical reproductive privacy is, and what relationships between different actors, technologies, and identity facets researchers, policymakers, technologists, and designers must consider. Still, we can look at existing efforts addressing this issue. The shield law policies [10] that some states have been pursuing are a good start for preventing technology companies and data brokers from creating or sharing reproductive health-related information. Yet they are inadequate to shield PCOPs from investigations of their data on their phones—a notably critical vector as we have seen in cases even before Roe [86]. Future work may explore how technology and policy might be designed to support sociotechnical reproductive privacy in volatile reproductive rights landscapes. While policies protecting against certain types of warranted searches may be critical, as HCI scholars,

[8]Efforts to manage one's reproductive privacy concerns in light of threats and legislation criminalizing reproductive experiences [37, 81] increases the labor of a community (e.g., PCOP) already investing much time, resources and energy into managing their reproductive healthcare, and experiences across their lifespans [46].

we strongly urge technology companies to consider ways to create more features that normalize encryption, expiring messages, and expiring data.

5.4 Refusal, Regulation or Something Else Entirely? A Question Demanded by Legislative Instability

As we grapple with how PCOPs may navigate privacy threats and growing legislative uncertainty, we argue it might be reasonable for some to abstain from technology to mitigate reproductive privacy risks, even if it comes with certain trade-offs—e.g., to convenience, information seeking, and safety. Individuals may refuse technology in a variety of ways to resist privacy threats. These acts of refusal are what Gangadharan refers to as a type of *digital exclusion* [36] where "members of marginalized groups assert their agency in the face of structural injustice and refuse technology in different ways in order to develop and determine their own technologically mediated lives." However, it should not rest on PCOPs alone to have to bear the responsibility of managing sociotechnical reproductive privacy threats, especially if that means they are denied access to technologies necessary to live in the 21st century in the U.S. PCOPs in a post-Roe U.S., thus, face an ethical dilemma when it comes to existing in a society where technology might act as sites of both refusal and resistance for the sake of sociotechnical reproductive privacy, while also acting as weapons of surveillance and control.

We see opportunities at the state level for policy changes to be implemented to protect people's sociotechnical reproductive privacy. For example, following the overturning of *Roe v. Wade*, California implemented a series of interstate shield laws protecting those who helped abortion seekers from legal repercussions by out-of-state authorities, as well as enacting data privacy protections that prevent businesses from collecting, storing, or selling location data or personally identifying information about people frequenting or close by to family planning centers [10]. However, the efficacy of any given state policy that aims to protect PCOPs and their support networks remains unclear as other states pursue litigation and establish counter laws that may allow authorities to reach across state lines [7]. Uncertainties surrounding data surveillance and criminal liability thus make policy a partly unreliable solution, exacerbated by the uncertainty rampant in the U.S. political arena (e.g., Presidential election, Supreme Court cohort). As a result, States and policymakers are navigating uncertainty themselves, using legislation as shields against moving targets. While we do not think that all policy efforts are futile, we do think they are not end-all, permanent solutions. The overturning of *Roe v. Wade* itself is an exemplar of that.

Despite this, we posit that both policy and technical interventions are still needed to curb the misleading presentation of privacy perpetuated by technology companies, while simultaneously pursuing more stringent data privacy protections. Future work can use the dimensions of sociotechnical reproductive privacy as a tool to guide interventions and support the design of policy and technology. Mapping out privacy risks, harms, and the dynamic relationships between, designers, and policymakers may be supported in identifying opportunities to effectively intervene.

6 CONCLUSION

Under the increasingly precarious landscape of reproductive rights in the post-Roe U.S., we examined the reproductive privacy concerns of people with the capacity for pregnancy (PCOP) and the strategies they use to mitigate these concerns. We found that PCOPs feel a lack of control over their reproductive health information and are concerned about the possible legal and social consequences if their data were accessed by actors with the authority to inflict harm or take punitive measures. We also highlight a range of low- and high-tech strategies employed by PCOPs designed to obfuscate or minimize their reproductive health-related digital footprints and protect their privacy. We demonstrate how PCOPs' reproductive privacy concerns and technology strategies are a response

to complex and shifting relationships between themselves and their perceived vulnerabilities to reproductive privacy threats.

Building from our analysis, we offer a conceptual framework of *Sociotechnical Reproductive Privacy* to make sense of privacy issues pertaining to data that may be perceived as relevant to, or indicative of individuals' reproductive decisions and experiences. This framework highlights how such data and individuals' autonomy over their reproductive decisions and experiences can be both threatened and safeguarded through the interplay of three dimensions: actors, technology, and identity. We introduce the term *reproductive privacy labor* to characterize the safety and data work individuals perform to manage their sociotechnical reproductive privacy in an era characterized by the policing of motherhood, criminalization of pregnancy, and surveillance of PCOPs. We conclude by 1) reflecting on the ethics of technology companies' ethos of data permanence in a world where digital footprints relating to reproductive health endanger PCOPs, and 2) discussing the limits of regulation when what we are trying to regulate is constantly metamorphizing into new sociotechnical reproductive privacy threats.

7 ACKNOWLEDGMENTS

This work was partially supported by the National Science Foundation (award #2309275 and award #2309278). We would like to thank participants for sharing their perspectives and experiences. We are also grateful to the ACs and anonymous reviewers for their constructive feedback. We also express our deep gratitude to Alan Luo for his guidance and help in using an open-source transcribing software. The first author also would like to express thanks to her two cats, Mishmish and Yeimy, who remained (mostly) silent during participant interviews and carefully supervised the writing of this manuscript.

REFERENCES

[1] 1996. Health Insurance Portability and Accountability Act.

[2] 2022. Dobb v. Jackson Women's Health Organization. , 19–1392 pages. Issue: No. 496 Publication Title: US.

[3] ACLU. [n. d.]. Surveillance Under the Patriot Act. https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act

[4] 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 Adjunct)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3547522.3547674 event-place: Aarhus, Denmark.

[5] 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*. ACM, Portland Oregon USA, 1485–1500. https://doi.org/10.1145/2998181.2998243

[6] Eric P.S. Baumer and M. Six Silberman. 2011. When the implication is not to design (technology). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Vancouver BC Canada, 2271–2274. https://doi.org/10.1145/1978942.1979275

[7] Aria Bendix. 2023. Idaho becomes one of the most extreme anti-abortion states with law restricting travel for abortions. https://www.nbcnews.com/health/womens-health/idaho-most-extreme-anti-abortion-state-law-restricts-travel-rcna78225

[8] Eric Berkowitz. 2015. *The Boundaries of Desire: A Century of Good Sex, Bad Laws, and Changing Identities*. Catapult.

[9] Suzanne Bernstein. 2024. The Role of Digital Privacy in Ensuring Access to Abortion and Reproductive Health Care in Post-Dobbs America. https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/technology-and-the-law/the-role-of-digital-privacy-in-ensuring-access-to-reproductive-health-care/

[10] Natalie Birnbaum. 2023. AHLA - SB 345: California's Abortion Shield Law and the Potential Impact on Medication Abortion Access Nationwide. https://www.americanhealthlaw.org/content-library/health-law-weekly/article/cfecb23f-5083-42f7-aa64-f76629905a5d/sb-345-california-s-abortion-shield-law-and-the-po

[11] Sarah Brayne. 2020. Dragnet Surveillance: Our Incriminating Lives. In *Predict and Surveil* (1 ed.). Oxford University PressNew York, 37–55. https://doi.org/10.1093/oso/9780190684099.003.0003

[12] Urie Bronfenbrenner. 1992. Ecological systems theory. In *Six theories of child development: Revised formulations and current issues*. Jessica Kingsley Publishers, London, England, 187–249.

[13] Finn Brunton and Helen Nissenbaum. 2016. *Obfuscation: a user's guide for privacy and protest* (first mit press paperback edition ed.). The MIT Press, Cambridge, Massachusetts London.

[14] Peter J. Burke and Jan E. Stets. 2009. *Identity theory*. Oxford Univ. Press, New York, NY.

[15] Albert Fox Cahn and Eleni Manis. 2022. Pregnancy Panopticon. https://www.stopspying.org/pregnancy-panopticon

[16] Jiaxun Cao, Hiba Laabadli, Chase Mathis, Rebecca Stern, and Pardis Emami-Naeini. 2024. "I Deleted It After the Overturn of Roe v. Wade": Understanding Women's Privacy Concerns Toward Period-Tracking Apps in the Post Roe v. Wade Era. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*. ACM, New York, NY, USA, 22. https://doi.org/10.1145/3613904.3642042

[17] Morgan Carmen. 2023. Abortion Snitching Is Already Sending People to Jail. https://msmagazine.com/2023/08/19/celeste-burgess-abortion-snitching-privacy-police-illegal/

[18] Alice F Cartwright, Mihiri Karunaratne, Jill Barr-Walker, Nicole E Johns, and Ushma D Upadhyay. 2018. Identifying National Availability of Abortion Care and Distance From Major US Cities: Systematic Online Search. *Journal of Medical Internet Research* 20, 5 (May 2018), e186. https://doi.org/10.2196/jmir.9717

[19] Center for Reproductive Rights. 2024. Alliance for Hippocratic Medicine v. FDA. https://reproductiverights.org/case/alliance-for-hippocratic-medicine-v-fda/

[20] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–20. https://doi.org/10.1145/3491102.3517475

[21] Danielle K Citron. 2023. Intimate Privacy in a Post-Roe World. *Florida Law Review* 75, 6 (Nov. 2023), 1033–1071.

[22] Juliet M. Corbin and Anselm L. Strauss. 2015. *Basics of qualitative research: techniques and procedures for developing grounded theory* (fourth edition ed.). SAGE, Los Angeles.

[23] Kimberle Crenshaw. 1991. Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Review* 43, 6 (July 1991), 1241. https://doi.org/10.2307/1229039

[24] David Shepard and Mamie Bittner. 2010. First-Ever National Study: Millions of People Rely on Library Computers for Employment, Health, and Education. https://www.gatesfoundation.org/ideas/media-center/press-releases/2010/03/millions-of-people-rely-on-library-computers-for-employment-health-and-education

[25] Jolynn Dellinger and Stephanie Pell. 2024. Bodies of Evidence: The Criminalization of Abortion and Surveillance of Women in a Post-Dobbs World | Duke Journal of Constitutional Law & Public Policy. *Duke Journal of Constitutional Law & Public Policy* 19 (April 2024).

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

[27] Paul Dourish. 2006. Implications for design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Montréal Québec Canada, 541–550. https://doi.org/10.1145/1124772.1124855

[28] Nadine El-Bawab. 2022. Indiana's attorney general files complaint against doctor who gave 10-year-old an abortion. *ABC News* (Dec. 2022). https://abcnews.go.com/US/indianas-attorney-general-files-complaint-doctor-gave-child/story?id=94215243

[29] Nadine El-Bawab. 2022. Nebraska mother, daughter charged for illegal abortion after police obtain Facebook messages. *ABC News* (Aug. 2022). https://abcnews.go.com/US/nebraska-mother-daughter-charged-illegal-abortion-police-obtain/story?id=88191900

[30] Elizabeth Nash. 2021. For the First Time Ever, U.S. States Enacted More Than 100 Abortion Restrictions in a Single Year. https://www.guttmacher.org/article/2021/10/first-time-ever-us-states-enacted-more-100-abortion-restrictions-single-year

[31] Elizabeth Nash and Sophia Naide. 2021. State Policy Trends at Midyear 2021: Already the Worst Legislative Year Ever for U.S. Abortion Rights | Guttmacher Institute. https://www.guttmacher.org/article/2021/07/state-policy-trends-midyear-2021-already-worst-legislative-year-ever-us-abortion

[32] Mabel Felix, Laurie Sobel, and Alina Salganicoff Published. 2024. The Comstock Act: Implications for Abortion Care Nationwide. https://www.kff.org/womens-health-policy/issue-brief/the-comstock-act-implications-for-abortion-care-nationwide/

[33] Jill Filipovic. 2024. How American Women Could Lose the Right to Birth Control. https://time.com/6977434/birth-control-contraception-access-griswold-threat/

[34] Diana Greene Foster. 2021. *The Turnaway Study: Ten years, a Thousand Women, and The Consequences of Having–or Being Denied–An Abortion* (first scribner trade paperback edition ed.). Scribner, New York London Toronto Sydney New Delhi.

[35] Jocelyn Frye, Shaina Goodman, and Areeba Haider. 2024. Democracy & Abortion Access: Restrictive Voting Laws Across States Threaten Freedoms. https://nationalpartnership.org/report/democracy-abortion-access-restrictive-voting-laws-across-states-threaten-freedoms/

[36] Seeta Gangadharan. 2021. Digital exclusion: A politics of refusal. *Digital technology and democratic theory* (2021), 113–140. Publisher: University of Chicago Press Chicago.

[37] Michele Goodwin. 2020. *Policing the Womb: Invisible Women and the Criminalization of Motherhood*. Cambridge University Press, Cambridge, United Kingdom ; New York, NY, USA.

[38] Alison Griswold. [n. d.]. Uber drivers are filming their riders and sharing the tapes online. https://qz.com/985832/uber-drivers-are-filming-their-riders-with-dash-cams-to-protect-against-bad-reviews-and-false-accusations/ Publication Title: Quartz.

[39] Jessica Smartt Gullion. 2018. Assemblages and Entanglements. In *Diffractive ethnography: social sciences and the ontological turn*. Routledge, Taylor & Francis Group, New York London, 105–118.

[40] Guttmacher Institute. [n. d.]. Interactive Map: US Abortion Policies and Access After Roe. https://states.guttmacher.org/policies/

[41] 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*. ACM, Vancouver BC Canada, 1176–1190. https://doi.org/10.1145/2675133.2675152

[42] Casey Michelle Haining, Louise Anne Keogh, and Julian Savulescu. 2022. The Unethical Texas Heartbeat Law. *Prenatal Diagnosis* 42, 5 (May 2022), 535–541. https://doi.org/10.1002/pd.6136

[43] Kashmir Hill. 2022. Deleting Your Period Tracker Won't Protect You. *The New York Times* (June 2022). https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html

[44] Grace E. Howard. 2024. *The Pregnancy Police: Conceiving Crime, Arresting Personhood*. Number 10 in Reproductive Justice: A New Vision for the 21st Century. University of California Press.

[45] Jane Im, Sarita Schoenebeck, Marilyn Iriarte, Gabriel Grill, Daricia Wilkinson, Amna Batool, Rahaf Alharbi, Audrey Funwie, Tergel Gankhuu, Eric Gilbert, and Mustafa Naseem. 2022. Women's Perspectives on Harm and Justice after Online Harassment. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (Nov. 2022), 355:1–355:23. https://doi.org/10.1145/3555775

[46] Grazyna Jasienska. 2017. Costs of Reproduction, Health, and Life Span in Women. In *The Arc of Life: Evolution and Health Across the Life Course*, Grazyna Jasienska, Diana S. Sherry, and Donna J. Holmes (Eds.). Springer New York, New York, NY, 159–176. https://doi.org/10.1007/978-1-4939-4038-7_10

[47] Nadia Karizat, Dan Delmonaco, Motahhare Eslami, and Nazanin Andalibi. 2021. Algorithmic folk theories and identity: How TikTok users co-produce Knowledge of identity and engage in algorithmic resistance. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–44. ISBN: 2573-0142 Publisher: ACM New York, NY, USA.

[48] Liz Kelly. 2011. Standing the test of time? Reflections on the concept of the continuum of sexual violence. In *Handbook on Sexual Violence*, Jennifer Brown and Sandra Walklate (Eds.). Routledge, 17–26. Pages: xvii-xxvi Publication Title: Handbook on Sexual Violence.

[49] Os Keyes, Burren Peil, Rua M. Williams, and Katta Spiel. 2020. Reimagining (Women's) Health: HCI, Gender and Essentialised Embodiment. *ACM Transactions on Computer-Human Interaction* 27, 4 (Aug. 2020), 1–42. https://doi.org/10.1145/3404218

[50] René Kladzyk. 2023. Policing Gender: How Surveillance Tech Aids Enforcement of Anti-Trans.... https://www.pogo.org/investigations/policing-gender-how-surveillance-tech-aids-enforcement-of-anti-trans-laws

[51] Josia Klein and Sharita Gruberg. 2023. Bans on Abortion and Gender-Affirming Care Harm the LGBTQ+ Community. https://nationalpartnership.org/bans-abortion-gender-affirming-care-harm-lgbtq-community/

[52] Alison Lefkovitz. 2011. Men in the house: race, welfare, and the regulation of men's sexuality in the United States, 1961-1972. *Journal of the History of Sexuality* 20, 3 (2011), 594–614. Publisher: University of Texas Press.

[53] Alex Jiahong Lu, Tawanna R. Dillahunt, Gabriela Marcu, and Mark S. Ackerman. 2021. Data Work in Education: Enacting and Negotiating Care and Control in Teachers' Use of Data-Driven Classroom Surveillance Technology. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct. 2021), 1–26. https://doi.org/10.1145/3479596

[54] Marcus Ma, Chae Hyun Kim, Kaely Hall, and Jennifer G. Kim. 2023. It Takes Two to Avoid Pregnancy: Addressing Conflicting Perceptions of Birth Control Pill Responsibility in Romantic Relationships. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW2 (Sept. 2023), 1–27. https://doi.org/10.1145/3610073

[55] Alex Leeds Matthews and Curt Merrill. 2023. One year without Roe: How the Frenzy of Legal Actions Shifted the Landscape of Access to Abortion. *CNN* (June 2023). https://www.cnn.com/interactive/2023/06/us/abortion-timeline-roe-overturned/

[56] Tobias Matzner, Philipp K. Masur, Carsten Ochs, and Thilo Von Pape. 2016. Do-It-Yourself Data Protection—Empowerment or Burden? In *Data Protection on the Move*, Serge Gutwirth, Ronald Leenes, and Paul De Hert (Eds.). Vol. 24. Springer Netherlands, Dordrecht, 277–305. https://doi.org/10.1007/978-94-017-7376-8_11 Series Title:

Law, Governance and Technology Series.
[57] Nora McDonald and Nazanin Andalibi. 2023. "I Did Watch 'The Handmaid's Tale'": Threat Modeling Privacy Post-roe in the United States. *ACM Transactions on Computer-Human Interaction* 30, 4 (Aug. 2023), 1–34. https://doi.org/10.1145/3589960
[58] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–14. https://doi.org/10.1145/3313831.3376167
[59] 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*. ACM, Yokohama Japan, 1–11. https://doi.org/10.1145/3411764.3445132
[60] Maryam Mehrnezhad and Teresa Almeida. 2023. ""My sex-related data is more sensitive than my financial data and I want the same level of security and privacy\": User Risk Perceptions and Protective Actions in Female-oriented Technologies". In *Proceedings of the 2023 European Symposium on Usable Security*. ACM, Copenhagen Denmark, 1–14. https://doi.org/10.1145/3617072.3617100
[61] 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*. ACM, Karlsruhe Germany, 145–150. https://doi.org/10.1145/3549015.3554204
[62] Nidhi Nellore and Michael Zimmer. 2023. Femtech Data Privacy Post-Dobbs: A Preliminary Analysis of User Reactions. In *Computer Supported Cooperative Work and Social Computing*. ACM, Minneapolis MN USA, 226–228. https://doi.org/10.1145/3584931.3606986
[63] Alfred Ng. 2024. A company tracked visits to 600 Planned Parenthood locations for anti-abortion ads, senator says. https://www.politico.com/news/2024/02/13/planned-parenthood-location-track-abortion-ads-00141172
[64] Trine Rask Nielsen, Maria Menendez-Blanco, and Naja Holten Møller. 2023. Who Cares About Data? Ambivalence, Translation, and Attentiveness in Asylum Casework. *Computer Supported Cooperative Work (CSCW)* 32, 4 (Dec. 2023), 861–910. https://doi.org/10.1007/s10606-023-09474-7
[65] Fay Cobb Payton. 2003. Rethinking the digital divide. *Commun. ACM* 46, 6 (June 2003), 89–91. https://doi.org/10.1145/777313.777318
[66] Kathleen Pine, Claus Bossen, Naja Holten Møller, Milagros Miceli, Alex Jiahong Lu, Yunan Chen, Leah Horgan, Zhaoyuan Su, Gina Neff, and Melissa Mazmanian. 2022. Investigating Data Work Across Domains: New Perspectives on the Work of Creating Data. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems (CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3491101.3503724
[67] Enrico Maria Piras. 2019. Beyond self-tracking: Exploring and unpacking four emerging labels of patient data work. *Health Informatics Journal* 25, 3 (Sept. 2019), 598–607. https://doi.org/10.1177/1460458219833121
[68] Planned Parenthood. [n. d.]. What's the Plan B morning-after pill? https://www.plannedparenthood.org/learn/morning-after-pill-emergency-contraception/whats-plan-b-morning-after-pill
[69] Planned Parenthood. 2024. Roe v. Wade: Behind the Case That Established the Legal Right to Abortion. https://www.plannedparenthoodaction.org/issues/abortion/roe-v-wade/roe-v-wade-behind-case-established-legal-right-abortion
[70] Layla Quran, Maea Lenei Buhre, and Amna Nawaz. 2024. The increasing risk of criminal charges for women who experience a miscarriage. *PBS NewsHour* (Jan. 2024). https://www.pbs.org/newshour/show/the-increasing-risk-of-criminal-charges-for-women-who-experience-a-miscarriage
[71] Lara Reime, Vasiliki Tsaknaki, and Marisa Leavitt Cohn. 2023. Walking Through Normativities of Reproductive Bodies: A Method for Critical Analysis of Tracking Applications. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–15. https://doi.org/10.1145/3544548.3581450
[72] Loretta Ross and Rickie Solinger. 2017. *Reproductive Justice: An Introduction*. Number 1 in Reproductive justice : a new vision for the twenty-first century. University of California Press, Oakland, California.
[73] Shruti Sannon and Dan Cosley. 2019. Privacy, Power, and Invisible Labor on Amazon Mechanical Turk. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300512
[74] Shruti Sannon and Andrea Forte. 2022. Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (Nov. 2022), 1–33. https://doi.org/10.1145/3555556
[75] Ari Schlesinger, W. Keith Edwards, and Rebecca E. Grinter. 2017. Intersectional HCI: Engaging Identity through Gender, Race, and Class. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, Denver Colorado USA, 5412–5427. https://doi.org/10.1145/3025453.3025766
[76] Joshua Sharfstein. 2024. The Alabama Supreme Court's Ruling on Frozen Embryos. *Bloomberg School of Public Health* (Feb. 2024). https://publichealth.jhu.edu/2024/the-alabama-supreme-courts-ruling-on-frozen-embryos

[77] Seward Sheraden. 2023. The Comstock Law (1873). https://hdl.handle.net/10776/1761
[78] Carter Sherman. 2024. 'I didn't know what I was supposed to do': US women who miscarry are in dangerous legal limbo post-Roe. *The Guardian* (Jan. 2024). https://www.theguardian.com/society/2024/jan/24/us-miscarriage-laws-abortion-rights-options
[79] Natasha Singer and Brian X. Chen. 2022. In a Post-Roe World, the Future of Digital Privacy Looks Even Grimmer. *The New York Times* (July 2022). https://www.nytimes.com/2022/07/13/technology/personaltech/abortion-privacy-roe-surveillance.html
[80] Julie Carr Smyth. 2023. A Black woman was criminally charged after a miscarriage. It shows the perils of pregnancy post-Roe. *AP News* (Dec. 2023). https://apnews.com/article/ohio-miscarriage-prosecution-brittany-watts-b8090abfb5994b8a23457b80cf3f27ce
[81] Rickie Solinger. 2019. *Pregnancy and Power: A History of Reproductive Politics in the United States* (revised edition ed.). New York University Press, New York.
[82] Daniel J Solove. 2021. The myth of the privacy paradox. *Geo. Wash. L. Rev.* 89 (2021), 1. Publisher: HeinOnline.
[83] Susan Leigh Star and Anselm Strauss. 1999. Layers of Silence, Arenas of Voice: The Ecology of Visible and Invisible Work. *Computer Supported Cooperative Work (CSCW)* 8, 1 (March 1999), 9–30. https://doi.org/10.1023/A:1008651105359
[84] Cella M Sum, Anh-Ton Tran, Jessica Lin, Rachel Kuo, Cynthia L Bennett, Christina Harrington, and Sarah E Fox. 2023. Translation as (Re)mediation: How Ethnic Community-Based Organizations Negotiate Legitimacy. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–14. https://doi.org/10.1145/3544548.3581280
[85] Yuling Sun, Xiaojuan Ma, Silvia Lindtner, and Liang He. 2023. Data Work of Frontline Care Workers: Practices, Problems, and Opportunities in the Context of Data-Driven Long-Term Care. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (April 2023), 1–28. https://doi.org/10.1145/3579475
[86] Jia Tolentino. 2022. We're Not Going Back to the Time Before Roe v. Wade. We're Going Somewhere Worse | The New Yorker. (June 2022). https://www-newyorker-com/magazine/2022/07/04/we-are-not-going-back-to-the-time-before-roe-we-are-going-somewhere-worse
[87] U.S. Department of Health and Human Services. 2024. HIPAA Privacy Rule Final Rule to Support Reproductive Health Care Privacy: Fact Sheet. https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/final-rule-fact-sheet/index.html Last Modified: 2024-04-22T15:05:02-0400.
[88] Aditya Vashistha, Abhinav Garg, Richard Anderson, and Agha Ali Raza. 2019. Threats, Abuses, Flirting, and Blackmail: Gender Inequity in Social Media Voice Forums. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Glasgow Scotland Uk, 1–13. https://doi.org/10.1145/3290605.3300302
[89] Fiona Vera-Gray. 2016. Situating Agency. https://www.troubleandstrife.org/2016/05/situating-agency/
[90] Katie Watson. 2018. *Scarlet A: The Ethics, Law & Politics of Ordinary Abortion.* Oxford University Press, New York.
[91] Cat Zakrzewski, Pranshu Verma, and Claire Parker. 2022. Texts, web searches about abortion have been used to prosecute women. *Washington Post* (July 2022). https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/

A INTERVIEW PROTOCOL

Thank you so much for agreeing to do this interview! [Review consent, Get Verbal Consent]
Tell me about yourself. What do you do day-to-day?

We asked to talk to you today because we wanted to learn more about how you are thinking about your privacy and health-related experiences, such as when seeking out healthcare.

(1) Could you tell me about a recent time that you were visiting the doctor or other health provider that you had concerns about your privacy, either *because of the* provider or that *you brought up with* your provider?
(2) When you have had those types of concerns, who [else] have you talked to about them? Probe: Family, friends, Spouse, etc?
(3) Did you seek out information about your privacy online?
(4) Did you ever share things or concerns about your privacy online?
(5) What type of help or information have you/did you receive? Was it helpful? Explain.
(6) Is there anywhere or anyone that you have reservations about sharing these concerns with? Probe: Family, Friends, Doctor or other healthcare provider, Spouse, etc?
(7) Have these concerns you just described affected the way you usetechnology? Probes:

- Social media
- Online support groups
- Online search
- What sites you visit
- What information you give
- How you shop online
- Your web browser, other tools?
- Tracking apps (e.g., menstrual, other wellness apps)
- Text
- Email
- What about the devices you use? (Probes: Work computers? Has this changed the way you use the library more/less? Why?)
- What about where you go with your devices?
- Other technology-related changes we haven't discussed?

(8) Thinking about these changes you just described, where did you go for advice about what to change? Probes: How did you realize you wanted to make these changes? Who or what influenced you to make these sorts of changes?
(9) How did you come across these resources that provided advice about tech use? Probe sources for *specific changes*: News articles, social media, friends, family, etc.
(10) Taking a step back, are there any other resources you've used or found helpful when trying to learn about how to protect your privacy? What are they? How did you find them? What caused you to trust those resources for guidance?
(11) Has your doctor ever asked about how you wanted to share your medical records? How did that conversation come up? What did you decide? What led you to that decision?
(12) Are you familiar with the laws in your state that govern healthcare privacy? Listen and probe, remind them that you don't know and were just wondering.
(13) What is your sense of how those laws might be implemented? Probe: How does that affect how you use technology? Where you seek out health information? Whom you talk to?
(14) Do you have a sense of what that means for you?
(15) Do any of these laws affect how you use technology?

Is there anything else that I should know about you or your experience that is relevant to this discussion that we haven't talked about? Are there things that have changed that might be relevant that we haven't touched on?

Thank You [End Recording] and Honorarium

Received July 2024; revised December 2024; accepted March 2025