"I Did Watch 'The Handmaid's Tale'": Threat Modeling Privacy Post-Roe in the United States

Nora McDonald

George Mason University, nmcdona4@gmu.edu

Nazanin Andalibi

University of Michigan, andalibi@umich.edu

Now that the protections of Roe v. Wade are no longer available throughout the United States, the free flow of personal data can be used by legal authorities to provide evidence of felony. However, we know little about how impacted individuals approach their reproductive privacy in this new landscape. We conducted interviews with 15 individuals who may get/were pregnant to address this gap. While nearly all reported deleting period tracking apps, they were not willing to go much further, even while acknowledging the risks of generating data. Quite a few considered a more inhospitable, *Handmaid's Tale* like climate in which their medical history and movements would put them in legal peril but felt that, by definition, this reality was insuperable, and also that they were not the target—the notion that privileged location, stage of life did not make them the focus of government or vigilante efforts. We also found that certain individuals (often younger and/or with reproductive risks) were more attuned to the need to modify their technology or equipped to employ high and low-tech strategies. Using an intersectional lens, we discuss implications for media advocacy and propose privacy intermediation to frame our thinking about reproductive privacy.

CCS CONCEPTS • Human-centered computing~Human computer interaction (HCI)~Empirical studies in HCI•Security and privacy~Human and societal aspects of security and privacy

Additional Keywords and Phrases: reproductive health, pregnancy, surveillance, intimate data

1 INTRODUCTION

Caution: this paper includes topics related to sexual violence and pregnancy loss which may be distressing to readers.

The decision by the Supreme Court of the United States (US) in June 2022 to overturn Roe v. Wade, took away the constitutional protection of the right to abortion[1], leaving it to the states to decide whether to protect or restrict and criminalize abortion. In some states, bans immediately went into effect [40,90] while in others, bans are working their way through state judiciary, even if experiencing obstacles in the courts (e.g., [106]). This ruling in Dobbs v. Jackson Women's Health Organization[2] immediately raised concerns about reproductive privacy[3] and the fear of prosecution using people's digital traces and data.

A prevalent immediate response by some academics, journalists, advocates, and providers was to warn people off "period tracking apps" (e.g., [102]). But advocacy groups such as the Electronic Frontier

[1] We use the term "abortion" to encompass both a desired ending of a pregnancy as well as a range of procedures that some might not consider an abortion per se but in which the fetus is not viable. For example, an "ectopic pregnancy," as well as other later-term circumstances in which the fetus is not viable and presents a risk to the life of the pregnant person. Notably, when we are talking about disposing of embryos, we specify that.

[2] Dobbs v Jackson Women's Health is the Supreme Court decision in June of 2022 that asserts that the constitution of the United States does not protect the right to an abortion. The Dobbs v Jackson decision effectively overruled both Roe v. Wade (1973) and Planned Parenthood v. Casey (1992) (which upheld Roe v Wade) and gives individual states the right to choose how to regulate any aspect of abortion.

[3] In this paper we use "reproductive privacy" to refer to the set of activities and data that are connected with people's reproductive health (e.g., having Fibroids or Fragile X), pregnancy status, and history as it relates to pregnancy and pregnancy termination.

1073-0516/2023/1-ART1 $15.00
http://dx.doi.org/10.1145/3589960

Foundation (EFF) noted that the greatest threat was likely to be device searches resulting from healthcare providers, friends or family who report individuals who they suspect of abortion to law enforcement [49]. We have now seen (e.g., [75]) that should the US government subpoena messaging records from major social platforms about suspected violators, those platforms will comply. Overall, on the surface, the guidance to delete apps may have made intuitive sense as period tracking apps are used by millions of menstruating individuals worldwide [94] and they are extremely unscrupulous with data.

But there is more to reproductive privacy than what these apps capture. While the vulnerability of menstrual tracking apps is a cause for concern, their role as *the* vector for privacy violation may not provide the full picture of how privacy may be violated, or how people are made vulnerable to privacy threats and risks. For example, other data sources (like Google search and Facebook messenger) are more readily available and incriminating [57] and privacy advocacy and legal experts believe, based on their records, that tech companies will comply with warrants [99]. According to civil rights lawyers, text messages and search histories are most commonly used as evidence in prosecution of cases alleging feticide [92]. Credit cards are another source of data that are far more difficult to protect [64]. There are also, for example, companies like SafeGraph that are selling location data from Planned Parenthood facilities harvested from mobile apps—though they were banned from the Google Play Store, the implication is that safeguarding reproductive privacy against incursions by those seeking to prosecute is nearly impossible [32]. Given the concerns raised about digital and offline activity, and under a surveillance capitalist system [108], the space of technology and reproductive privacy risk is so large as to encompass, potentially anything one may say or do about their reproductive health. And while those data may not necessarily be subject to dragnets (depending on where one lives) once one comes under suspicion, they can become "evidence."

Clearly the need to defend reproductive privacy through technology regulation is important to our current government, as well as academics and citizens. During recent listening session with experts about technology platform's potential harms, the White House emphasized the need to implement "strong protections" on sensitive data, including reproductive health information about medical histories and choices that is collected or associated with where users are physically located [111]. Still, we know little about how individuals, who would most directly and personally be impacted by this ruling's implications for reproductive privacy, approach their privacy, particularly in interactions with technology—an exploration we undertake in this paper. We do so with a particular attention to intersectional vulnerability—consideration of factors like *reproductive risk* (e.g., how likely to get pregnant, have a miscarriage, have some other condition like Fragile X), which can also sometimes be, but not always, a proxy for *age* and *location*, which can make someone more or less prone to experiencing prosecution for criminal action or unwanted health outcomes as well as experience more repressive cultures and work environments; and other social and structural factors that contribute to someone's experience of privacy consequences (e.g., other trauma related to reproductive health). Many of these factors might intersect with marginality, which we consider to be the disadvantages experienced by those who are prevented from obtaining full membership and participation in society, often because of their race, ethnicity, gender, religion, sexual orientation, sexual identity [76]. Historically, marginality offers a window into privacy invasion and implications thereof that are not equally distributed; that is, surveillance (technologies) have

and continue to be used to profile and surveil marginalized groups (e.g., [39,41]). For marginalized women, surveillance risk and policing of pregnancy is anything but new [52]. Indeed, many marginalized people happen to be women, including low-income mothers [20] for whom, for example, the mere act of applying for public assistance for their children can subject them to pregnancy surveillance and presumptions of criminal intent. These presumptions are often used to justify invasions of their privacy. What has changed since Dobbs is the prosecutorial risks attached to those privacy violations as well as the scope of risk that now encompasses *all* individuals who may become pregnant.[4] For those newly made vulnerable to privacy risks, whatever encroachments were previously prepared to tolerate to live digital lives may now put them at grave risks and, by implication, might require them to rethink the tradeoffs of producing and sharing data about their reproductive health.

Although degree matters, one could argue that the political, economic, social, and legal vulnerabilities that people who may become pregnant now face contribute to marginalization to some degree as defined. Now, with anti-abortion legislation sweeping some states, all those of reproductive age capable of becoming pregnant in those states are likely to be subject to those same presumptions and more likely subject to risk if they, for example, are more likely to have a high-risk pregnancy. This expands and complicates the pool of vulnerability exponentially—even if the experience of being marginalized likely compounds vulnerability to new laws governing abortion. To explore these factors (some known and unknown) we adopt an intersectional interpretative lens based on Patricia Collins' matrix of domination [28] which emphasize the importance of context and power in relationship to a wide range of identities [29].

The overarching research question we address in this work is: *How (if at all) are individuals who may become physically pregnant thinking about privacy in relation to reproductive-related information following the decision to overturn Roe v. Wade?*

To answer this question, we conducted interviews with 15 cisgender women[5], for whom the loss of Roe v. Wade protections has direct implications, in order to examine how they understand their privacy risks and the strategies they develop to protect their reproductive privacy. The research we report on in this paper gives us a first glimpse into how (1) those who were already vulnerable (or at least are familiar with privacy violations because of their identity) and (2) those, more privileged, whose privacy risks have suddenly been escalated beyond intrusion to the potential for legal adjudication, are adjusting their risk calculus to accommodate the sudden change in circumstances and the continuing uncertainty, even volatility, of the circumstances they face. We find that while participants were quick to delete their period tracking apps, mostly from learning that this is what they should do from journalists and social media, few were taking other steps to protect their online or offline privacy. Nevertheless, some participants still considered a *Handmaid's Tale* like reality in which their medical history and movements would put them in legal peril but felt helpless to do anything about their privacy and (perhaps partly rationalized) that they were not the target because their location, stage of life, and/or identity did not make them the focus of

[4] We use the term "people who may become pregnant" to encompass people who do not identify as "women" but who have a uterus and are biologically able to get pregnant. We use the term "women" where we cite others' work for accurate reflections of these works.
[5] This study was open to all individuals who may become pregnant, but our sample only included cisgender women with a range of sexual orientations.

government or vigilante efforts. We also found that certain individuals (often younger or with high reproductive risk) were more attuned to the need to modify their technology or equipped to employ no/low-tech strategies (including abstinence from technology and sex) and high-tech strategies (e.g., VPN). We conclude with discussion and recommendations for media and privacy researchers—offering a way of thinking about and acting on privacy management. We call this ***privacy intermediaries*** which is both a role and a way of thinking about privacy and offering privacy management in intersectional ways—not about literacy so much as mitigating vulnerabilities in way attuned to structures of power, culture, and context [28]. As an intersectional [27–29] ***lens***, privacy intermediation takes into account structural barriers and strategies available to individuals that are not based on technology privacy literacy but what is available to navigate threats. Intersectional privacy intermediary is a ***role*** that could be adopted by anyone (counselors, social workers, service providers, and researchers) providing support for individuals with intersectional privacy needs. This is in keeping with Patricia Collins notion of intersectionality as a framework as well as *a way of thinking and a praxis* [28]. Other paradigms exist in HCI for this approach, like Havron et al's. work providing consultation services to those experiencing intimate partner violence (IPV) [56].

Considering privacy as intersectional is not new [68,70]. However, what is perhaps less understood is first, that intersectionality depends on the context. We find that contrary to what would be expected, historically marginalized individuals (i.e., Black, Latino and/or LGBTQ+ individuals who represent over half of our sample) are not necessarily the ones most attuned to risk so much as those who are young, have greater reproductive risk and/or live in a repressive state. Second, although more understood [66], the digital privacy strategies of those who are at the bottom rungs of the intersectional ladder take into account power imbalance and thus opt for abstinence—both technological and sexual.

2 BACKGROUND

We review scholarship on mHealth privacy and privacy research related to reproductive health as well as issues of surveillance capitalism that inform and motivate this study.

2.1 Privacy research and technology in the reproductive space

When it comes to reproductive health technology (the term we use to broadly refer to apps and IoT that monitor ovulation, pregnancy, breastfeeding, menstrual cycles as well as mood, and other health data from which reproductive status can be gleaned) much focus on HCI has been on the benefits they offer and not their privacy implications. For example, some studies look at how to better support lower-income [25,77,78] and diverse populations [89] and those with other pregnancy challenges [8]. But reproductive technology are notorious for privacy vulnerabilities because they deal with medical data but are not regulated by health privacy laws in the US. Like other apps, they share data—in this case, sensitive data about reproductive health—with third parties. For example, a review of 23 of the most popular "women's mHealth apps" found that, among other privacy concerns (like behavior and location tracking), the vast majority share data with third parties [2]. Other recent study of "fertility tracking apps" [3,73] (also referred to as "menstruapps" [87]) that track people's reproductive cycle for the purposes of helping them predict their periods highlight how these apps capture more than just period data including, general

health, sex, pregnancy, and data about partners, children, and friends [3]; do not treat reproductive data as private; and use questionable tracking practices, for example initiating trackers before users interact with the app [87].

While reproductive technologies are notably not required to comply with the Health Insurance Portability and Accountability Act (HIPAA) which sets standards in the US that protect sensitive patient information, they have nonetheless demonstrated some *notable* vulnerabilities over the years, making them potential vectors for privacy violation in the post-Roe era. For example, the popular app Glow was the subject of a class action lawsuit in 2016 for major security vulnerabilities that would have allowed someone with no hacking skills to access users' personal data [10]. More recently, Flo Period & Ovulation Tracker was charged by the Federal Trade Commission with sharing information to third parties like Facebook, Google, and others [110]. Flo's privacy policy also stipulates that it will share information with police [49].

Reproductive technologies are thus a space where privacy concerns have rarely been front and center when it comes to how humans interact with them, even while concerns about their data flows abound. This speaks, perhaps, to HCI's complacency when it comes to privacy more generally.

2.2 Beyond reproductive technology: other concerns for reproductive privacy

Scholarship about reproductive health and technology beyond reproductive technology has examined social media use in relation to pregnancy journeys [4,5,7] including privacy concerns in sharing about stigmatized reproductive health complications [4] as well as pregnancy loss disclosures among LGBTQ individuals [81], and support seeking among peers for pregnancy [53]. A full review of the former is outside the scope of this paper. An investigation by Gizmodo in 2022 found that dozens of data brokers in the US sell data on pregnant people [105]. The investigators note that one company was found to be selling access to over 60 million users labeled as "Pregnant and Maternity Life Stage," while another was offering access to nearly 10 million devices labeled "pregnancy test kit" [105].

According to the Stop Surveillance Technology Oversight project (STOP) "[p]rosecutors will obtain geofence warrants to track those at reproductive health clinics, even clinics out of state. Investigators will use keyword search warrants to identify everyone searching for abortion clinics, abortifacients, and even medically accurate information about abortion care" [24].

Other data includes a "catalogue" of those using birth control [105]—a potential target in some states looking to restrict their use. These catalogs are presumably derived from purchasing information, suggesting that, under some circumstances, one need only use a credit card to reveal reproductive status—no reproductive technology app required. While some investigations note that reproductive technology apps have explicit rights to share their data with law enforcement (e.g., study by Forbes [19]), it is not clear, in a market capitalist system, that any of the companies profiling reproductive-related purchases owe their users a greater debt of privacy. Increasingly, a case can be made that the only way to keep reproductive health information safe is to avoid all use of digital tools and leave devices at home when engaging in activities related to reproductive health [88], which could be a lot of activities. Surveillance by third parties has become so pervasive that it is impossible to turn off or retreat from.

It might be argued that the current remedial approach, emphasizing the risk of specific apps and encouraging "abstinence" from a particular technology is narrowly focused on alleviating the symptomatic evidence of the ailment rather than the disease. The underlying problem is our surveillance capitalist society [31,108]. With so much at risk and so many threat vectors in play—e.g., most obviously, our google histories, our unencrypted conversations, our social interactions, our confidential records between healthcare providers, should they be subpoenaed— it is important to examine what those who may become pregnant at risk of reproductive surveillance actually conceive of those risks including the rich troves of data they are supplying to commerce and now, potentially, to legal systems.

2.3 Privacy research and literacy in HCI

Privacy research has, understandably, focused on how users behave *in a given* context—on a platform. A traditional approach to understanding user privacy has been to explore app(s) or platform(s) and how users engage with them—their privacy settings, use, etc.—to gauge exposure to threats and how users are (or are not) attuned to them. Take for example, this early study establishing the privacy paradox (the idea that people act in ways that are at odds with their privacy attitudes or intentions) as a cornerstone of platform based researcher exploring how teens were using social networks in ways that exposed them to risk to better understand these contradictions [9]. This framing has led to privacy literacy efforts like how to nudge [1,100,103] or persuade users [60]. Research into informal literacy has suggested that informal stories from personal networks have an impact on privacy behaviors [79,82], though it's not clear the extent to which these are simply people replicating guidance, not in an effort to thwart perceived threats.

Reflecting on engagement with privacy studies of this kind, it is understandable that researchers focused on behaviors in narrow arenas. In fact, Daniel Solove, in criticizing the privacy paradox, in particular, makes the argument that it is simply illogical to look at broad privacy attitudes and compare them with actions in a particular context [91]. Still, the post-Roe world presents an opportunity to reset our approach and consider that privacy research must contend with the Faustian bargain that we may have once been able to afford. But as researchers have pointed out, users now represent a constituency of resignation (i.e., prone to a "sense of helplessness" in the face of routine surveillance by companies) [36]. Indeed, more recent criticism from scholars like Draper and Turow suggest that the privacy paradox is the result of corporations promoting "digital resignation" [36]. According to a report by Turow et al., the more we know about laws and practices of online marketers the more resigned we are to accept their privacy violations [96].

This study's goal is to examine what types of strategies are being used by a population who are vulnerable to privacy violations because of (recent changes to) reproductive health laws in the US. First, it is not clear that those not experiencing immediate risk are not resigned as Draper and Turow suggest, in which case privacy literacy may not be what's needed. Second, it is not clear that literacy efforts are appropriately attuned to the needs of individuals to manage specific, intersectional privacy incursions where the surface area of risk might preclude nudging or stories and require nuanced strategies yet undefined. Privacy literacy research presumes a certain platform-centric focus on privacy settings and not the terrain of risk that might be encountered by someone who must worry about what they say and do across social and digital spaces—what this study explores.

2.4 Surveillance capitalism and the reproductive health market

What scholars call surveillance capitalism [107,108] which shares some similarities with data colonialism [30] both include the constant harvesting of personal data that normalizes the futility of "collective public anger" [36]. Surveillance capitalism has enabled decades worth of big data collection and prediction including around pregnancy. Expecting pregnant individuals are an incredibly valuable target market. Predicting their behavior to identify their delivery date down to the month is big business [37]. Keeping this information private requires such a massive effort as to be essentially unsustainable. Indeed, Vertesi found that while abstaining from web searches about expecting was not hard, using social media and purchasing products without leaving a trail—which requires, for example, sticking to cash, burner emails, prepaid cards, VPNs, and Amazon mail lockers—was not a supportable privacy practice [58,97].

While the technology policies and practices that undergird surveillance capitalism are a concern, so too is the growing sense that new laws around, for example, reproductive rights supercharge what Foucault conceptualized as the norm-abiding power of panoptic environments [45], in which the threat of surveillance gets instrumentalized through technology by people and institutions [44] and becomes what Foucault describes as a state of governmentality in which the governed take part in governing others. What role does HCI have when privacy covers terrain well beyond devices, to encompass the offline world? What roles do academics have when the laws prohibit certain activities?

2.4.1 Surveillance capitalism plus social control

Let's assume that law enforcement is not regularly sifting through apps or third party entities' data to identify and investigate those who may become pregnant who look suspicious, *even though, they can and are expected to in some states* [59]. One potentially major risk that is increasingly being discussed are family and friends and healthcare providers [49], vigilante-enforced abortion law [13], as well as activist organizations. The latter, so-called "crisis pregnancy centers," present huge risks [74]. These centers, which have managed to rise to the top of Google search, falsely claim to provide abortion services, luring people into their facilities to convince those who may become pregnant not to go through with their plans to terminate and capturing their data in the process. They advertise on social media as well, attempting to capture the data of teens seeking "pregnancy tests" and "abortion," which they do not provide [74]. They also use misinformation to lure more people in—for example, a well-known tactic is telling those who may become pregnant that an ultrasound is required in order to have an abortion and use other tactics to lure people in [74]. The worry is that if those who are pregnant who visit these centers online or in-person do not ultimately give birth, their data could be, in some states, handed over to prosecutors. In this supercharged Foucauldian world, entire organizations are set up and empowered by Google search to enforce reproductive law.

As noted in McDonald et al, privacy theories have long presumed that individuals are in charge of their privacy, or that collective norms can properly regulate privacy policies and practices of the technologies we use [68]. We and others [91] argue that this is not a productive model for thinking about people's privacy strategies. What is needed is an understanding of how different types of vulnerability map to different types of privacy strategies—and that those strategies are likely to be low or non-technical. It is impossible to impose "one size fits all" approach to reproductive privacy.

3 METHODS

3.1 Participant recruitment

In September of 2022, we posted calls for participation for our study on Twitter and on Craigslist in the District of Columbia (DC), Oklahoma, and Texas. The call invited people for whom the decision to overturn Roe v. Wade was personally relevant because they are (or could someday become) sexually active in ways that may lead to pregnancy; trying to conceive/are pregnant with or without IVF; and/or have other reproductive-related concerns.

We chose DC to reach a diverse set of participants with respect to race/ethnicity [23] and sexuality [48]. We chose Oklahoma [80] as an example of a state with the most strict abortion ban and Texas where abortion is also outlawed and in which the so-called "bounty law" has created additional complexity to privacy management [13,61,109].[6] We also shared the call with people from our professional and personal networks, asking them to distribute it to people they thought might be interested in participating. Our networks may also have drawn participants from other states where abortion was under threat, but no state laws had officially banned it yet. Ultimately, we got the most participants from Craigslist (see Table 1).

Prospective participants were invited to take a screener survey and submit their email (either their own or a more secure ProtonMail email they were invited to create for the study—we shared the link and told them it was an option). The screener survey confirmed eligibility if respondents said they (1) reside in the US, (2) were between 18 and 49, and (3) were able to become pregnant with or without fertility assistance. We chose only to speak with adults (i.e., 18 and over) because of the sensitive nature of this topic. We set the age limit at 49 because, even while there are individuals getting pregnant beyond the age of 49, most healthcare data about pregnancy stops before 50; we also note that older individuals that could not become pregnant (or for whom the risk of an unwanted pregnancy was not as great) may have mostly shared concerns about others' risk (e.g., their family members, friends) and not themselves. Additionally, we screened participants for reasons why the Roe decision was personally relevant (notably this was asked to be inclusive of those who had reproductive health risk), any privacy technology they used, age, location, gender, sexuality, race/ethnicity, income, education, and location. We sought a mix of participants to increase the diversity of our sample, particularly making sure to include historically marginalized identities along dimensions of sexuality, race, income, and education.

In all, 199 people took our screener survey from which we reached out to 32 people[7]. We were able to schedule an interview with 15 participants; those 17 whom we emailed but did not interview either did not respond or follow-up.

[6] A Texas Law known as SB 8 is called a "bounty law" (or "vigilante-enforced" abortion law) because it incentivizes citizens to sue anyone whom they believe has aided a person to get an illegal abortion.

[7] We were primarily concerned about spam, which resulted in filtering out a large number of participants. Spam can be hard to detect even when considering trends in the data. For instance, if we had a wave of participants from a specific location in the US who identified as a certain racial category with an email address that used a generic western-centric name like "BobSmith123" we did not reach out. Other reasons for not reaching out included, in a few cases: those who identified as cisgender men; email addresses that seemed spoofy; or if we had exhausted a category of participant based on their demographics.

Our interview sample of 15 participants includes 4 who self-describe as bisexual or queer, 4 as Black/African American, 3 as Asian or Pacific Islander, 3 as Hispanic or Latino/Latina/Latinx, 2 as Middle Eastern with overlap among those categories (see Table 1). Our sample includes one participant whom we are not sure was telling the truth about their identity; and we do not reflect their views except in the very few instances when they seem to emphasize others' views. We did our best to screen participants with our screener survey and at the beginning of the interviews and, with the exception noted, have no other doubts about participants who risked a lot to share their stories about their reproductive privacy and health.

We told survey respondents that we would reach out to them if they were selected to participate in the interview noting that we were looking for a diverse set of participants. All participants self-described as women, though the survey was open to everyone who could become pregnant who did not identify as a woman such as transgender men or non-binary individuals. We did not ask for pronouns out of concern that the practice would not be familiar to some of our participants and refer to participants, all of whom identify as women, as "she/they/them."

Table 1. Participant demographics, recruitment channel, and name assignment

Sexual orientation	Race/Eth	Age	Education	Low income	Int#	Pseudo	Location	Recruit.	Prof. field
Hetero	White	25 - 34	Professional degree (JD, MD)	No	INT1	Emily	Michigan	Twitter	Medicine
Hetero	White	35 - 49	Professional degree (JD, MD)	No	INT2	Elisa	Nevada	Email	Marketing
Hetero	Asian or Pac Isl.	35 - 49	BA	No	INT3	Stephanie	Maryland	Craigslist	Marketing
Hetero	Hispanic or Latinx	35 - 49	Master's	No	INT4	Lucy	DC	Craigslist	Knowledge adm
Bisexual	Black, Asian or Pac Isl.	18 - 24	Assoc degree	Yes	INT5	Rowan	DC	Craigslist	Childcare
Bisexual	White	25 - 34	Some college	Yes	INT6	Antonia	DC	Craigslist	Self employed
Hetero	White	35 - 49	Some college	Yes	INT7	Sharon	North Carolina	Craigslist	Mechanics
Questioning/Prefer self describe	White	35 - 49	Doctoral degree (PhD)	No	INT8	Victoria	Illinois	Twitter	Psychology/Academic
Bisexual, Gay/lesbian	Black	25 - 34	BA	Yes	INT9	Evette	Georgia	Friend	Fashion
Hetero	Middle Eastern	25 - 34	Master's	Yes	INT10	Rocky	Michigan	Twitter	Unemployed
Hetero	Black	35 - 49	Some college	No	INT11	Veronica	Virginia	Craigslist	Housewife

Questioning/Prefer self describe	Hispanic or Latinx, Black, White, Indian/Native American or Alaska Native	35 - 49	BA	No	INT12	Lily	Oklamhoma	Craigslist	Self employed
Hetero	Asian or Pac Isl.	35 - 49	Master's	No	INT13	Kim	Virginia	Unsure (Friend)	Cosmetics
Queer	White	35 - 49	PhD	No	INT14	Jessie	Missouri	Twitter (Friend)	Academic
Hetero	Hispanic or Latinx, White, Middle Eastern	25-34	BA	Yes	INT15	Sylvia	DC	Craigslist	Project management

3.1.1 Additional privacy considerations

While we attempted to include younger participants in our survey, the participants skew older. This is, we think, in part because of our extended professional networks and who might (not) be willing to speak on the record about such a sensitive topic that might put them at risk. That said, we took extra precaution to protect the privacy of our participants and while imperfect, included the following: 1) we offered them the option and link to create an encrypted email to correspond about the study; 2) when we reached out to them, our emails were cryptic and did not include any information about the study except our availability and that we would follow up with a zoom link; 3) we recorded on Zoom off video and asked that participants remove identifying photos or their full name; 4) we did not have participants sign a consent form, only verbal consent over Zoom following our review of the consent form over screenshare before the interview began; 5) we shared the honorarium ($30 amazon gift card) over non-recorded chat in Zoom; 6) we did not send out our recordings for transcription; and 7) we deleted participants' emails following the data collection completion.

3.2 Data collection

We conducted 15 interviews off-video over Zoom. All interviews were transcribed by Zoom, with additional editing by the first author. The consent and honorarium, as well as some more sensitive conversation was done off record. The recorded portion of the interviews were an average of 32 minutes and lasted between 13 minutes and 56 minutes. The interviews were a sufficient length to capture participants' context as it related to reproductive health and Roe as well as privacy technology strategies, and the context behind those decisions. It was also important to us to not gather any more data than we absolutely need because of the sensitive nature of this study within the US context. A third of our interviews where we recorded for 40 minutes to an hour, and in some of those cases, we would have like to have spoken with participants more but would have well exceeded the 60 minutes requested in our research call. One interview was conducted over both Zoom and other methods (not identified for privacy reasons) because of challenges with the participant's WiFi.

In our interviews, we asked participants to describe why the Supreme Court decision to overturn Roe v Wade was personally relevant and asked them to describe those circumstances/their reproductive health in the context of how they were sharing this information before and after the Supreme Court decision—asking specifically about changes to who they shared with and what technology they used. Interviews probed on how and why on examples that mostly they provided like period tracking, email, text, social media, health records and online health portals. Participants were also asked where they went for

sources/resources about any changes to their information sharing behavior; their familiarity with the laws in their state; and should they need an abortion, what would they do?

While we asked about technology use, we structured our conversation to avoid priming participants to think about technology risks. For instance, we asked what, if anything, had changed about their technology use but avoided probing about numerous technologies or devices or asking about it in negative terms.

3.3 Analysis

Following each interview the first author wrote memos, which would later become the vignettes in our findings. The first author conducted thematic analysis [15,17] by open coding concepts that would ultimately become the themes described in the findings. Themes represent patterns of codes in the data grouped into domains or concepts. They represent concepts that are most salient, not necessarily most frequently encountered—though we make clear in our findings when themes are based on salience rather than occurrence [16].

3.4 Interpretative lens and framing of results: Intersectionality, Privacy Intermediation and Use of Thicker Narrative

Intersectionality operates as a framework and methodology. While we approached this research with a phenomenological [85] stance, we employ intersectionality[27–29] as a frame for our analysis because it lends critical importance to thinking about power in relationship to multiple, interconnected social coordinates and vulnerabilities. One core insight of intersectionality is that "conditions of social and political life" are "not shaped by any one factor" but that they build on one another and one must explore these interconnections in relation to power [29]. In our work, the media, authorities, reproductive health workers, people's social and work networks, etc. all have power to influence privacy strategies. Understanding what it is individuals do, however, require a sensitivity to the multiple dimensions of experience. By looking at the interdependence of reproductive health risk, power, culture, and other facets of identity we aim to construct the type of nuanced view that we believe is an important orientation for privacy intermediation—a way of thinking about and ultimately providing holistic and integrative privacy management for those who are vulnerable and which we expand on in the discussion. To that end, while our results were derived using thematic analysis, we use details about participants ("thicker narrative") to provide some scene-setting and context for understanding nuanced privacy decisions, drawing inspiration from narrative techniques used in ethnography experiences that emphasize telling a "great" story by evoking images and feelings and communicating people's experiences [54].

In taking an intersectional lens to our interpretation, we draw heavily from black feminist scholar, Patricia Hill Collins. Collins puts forth the notion of the *matrix of domination* or intersecting vectors of power [26] to describe the way in which different groups, with different encounters with discipline and power and privilege, have only partial perspectives. Collins notably also posits intersectionality as a theory in the making—a "way of thinking" [28] and it is in that spirit that we adopt this lens and embrace the messiness of attempting to understand the extent to which experiences with a matrix of oppression and also what those matrix look like can sensitize HCI scholars and designers to non-normative ways of

thinking about privacy and risk as it relates to technology. To do that, we borrow from the core tenants of Collins' matrix of domination: ***interpersonal*** (how people's actions shape power relations), ***disciplinary*** (which rules apply, to whom, and when; e.g., bureaucratic organizations perform routine surveillance for the sake of efficiency), *hegemonic or* ***cultural*** (conditions under which power takes hold) and ***structural*** (how powerful institutions are organized; e.g., laws, policies, etc.) domains of power [26,28,29]. We map the construction of privacy imaginaries like the *Handmaid's Tale* on to hegemonic domains of power. Disciplinary domains and structural domains also map to tech company business logics and algorithms that fuel accumulation of data for advertising. That is, one of the ways that this matrix manifest is through surveillance capitalism/data colonialism, which reifies oppressions through advertising models, policies, and algorithmic surveillance that discriminates and disproportionately affects and harms certain marginalized groups. To grapple with this relational complexity, we looked to analytical approaches that have emerged from intersectional studies that focus on intercategorical thinking which requires that "scholars provisionally adopt existing analytical categories to document relationships of inequality among social groups and changing configurations of inequality along multiple and conflicting dimensions" [67].

We expected that because surveillance disproportionally impacts marginalized individuals (e.g., [18,21,38,39,41,42,84,86]) potentially affecting their interaction and agency with technology that they would indeed be more likely to adopt non-technological approaches—feeling that that they had no other options. But we were nevertheless not sure of how perceptions of technology and identity might interrelate, nor how they might affect participants not in traditionally marginalized groups. Surveillance studies offer researchers a way of thinking about the collective nature of privacy and the way that power influences agency [65].

4 FINDINGS

We set out to understand, for people who may get or were pregnant, how the Supreme Court decision to overturn Roe v. Wade has influenced the way they manage reproductive health information. While a few participants did not believe that they would ever choose abortion, all were against the decision to take away the right to have an abortion.

We found that, except for deleting their period tracking apps (or deciding not to use them), most participants are not using technology differently. The reasons for not taking steps given mostly had to do with a privileged stance—some combination of age or stage of life (e.g., being older and not the target of surveillance, possibly not as fertile or sexually active as in there 20's) and the laws in their state (if they do not outlaw abortion or ectopic pregnancies). This culminates in the feeling among participants that they are not the "target" for prosecutorial intervention—which one participant notably describes as "people who don't have anyone to advocate for them." Where we see more effort to protect reproductive privacy (or its consequences when it is violated) is among younger participants who often described no/low-tech methods for avoiding abortion (e.g., contraception, abstinence, body awareness, good judgement, etc.) and so were also not that worried about unwanted pregnancies. Those facing higher reproductive risk or in states with an abortion ban or experience of oppressive laws or social outlooks were also more concerned about privacy but may have been using more sophisticated technology strategies in combination with

no/low-tech (e.g., traveling, avoid bringing phones with them and/or not searching on the internet for clinics).

Regardless of whether they are taking steps to change their technology privacy management practices, participants still mention concerns about a dystopic reality and of "always being tracked," (pointing to advertising algorithms as an example), about geolocation and IP tracking, and "lists" of abortion seekers being created by conservative or right-wing religious organizations. This kind of thinking falls into what we—and often *they*—describe as *Handmaid's Tale* thinking. This mode of thought is entangled with notions of surveillance capitalism and authoritarianism—drawing its name from the dystopian television series adapted from the book by Margaret Atwood by the same name[8]. The reference evokes a kind of technological (and social) spying, an anything-goes-authoritarianism, and an idea of women as "vessels" for a white male dominated society to procreate. Notably, this thinking does not (with some noted exceptions for certain individuals) cause participants to act differently regarding their privacy and technology. Rather, it references a potential (maybe far off, maybe not) reality in which their every move is tracked and in which their womb is policed. Even those that don't explicitly evoke *The Handmaids' Tale* mostly acknowledge that the government is potentially always watching; and they feel somewhat resigned to being powerless in that reality, while also, paradoxically, being able to find an abortion if they need it. In our findings, we first explore participants' understanding of laws and technology risks. We then detail perceptions of risk and privacy strategies that overlap with sets of identity characteristics, circumstances, and relationships to power.

In our results we describe how certain overlapping categories: *reproductive risk* (e.g., how likely to get pregnant, have a miscarriage, have some other condition like Fragile X), which can also sometimes be, but not always, a proxy for *age* and *location*, which can make someone more or less prone to experiencing prosecution for criminal action or unwanted health outcomes, as well as experience more repressive cultures and work environments; and other social and structural factors that contribute to someone's experience of privacy consequences (e.g., other trauma related to reproductive health). These categories generally follow distinct patterns in terms of privacy strategies. Below we describe how intersectional risk and strategy relate and apply the power matrix framework used by Collins to consider how they map to domains of power.

- No abortion ban, low reproductive risk leads to a default *Handmaid's Tale* style thinking (4.1 and 4.2)
- Younger (**cultural** domain of power) /High reproductive risk (of getting pregnant) (**disciplinary** and **structural** domains of power) risk leads to no/low-tech technology privacy strategy (4.3)
- High reproductive risk (**disciplinary** and **structural** domains of power), location/law banning abortion (**structural** domain of power) or experience with oppressive states or environments (**cultural** and **interpersonal** domains of power) leads to mix no/low- and high-technology privacy strategy (4.4)

[8] *The Handmaid's Tale* is a dystopian novel by Canadian author Margaret Atwood set in a fictional totalitarian state called the Republic of Gilead that has overthrown the US government. In Gilead certain women are forced to serve as "handmaids" that produce children for the ruling class. *The Handmaid's Tale* was made into a TV series on the streaming service Hulu to major critical acclaim.

Mapping to Collin's domains of power: While we associate *being younger* with higher reproductive risk (of getting pregnant) it is also a **cultural** domain of power in that participants perceive that being younger makes one more of a target because people associate youth with fertility or that they must combat their risk by setting boundaries and defining their own norms about sex. Having a *high reproductive risk* is associated with **disciplinary** power because, for example, miscarriages might be viewed with different degrees of suspicion, depending on the clinic and have also **structural** power when there is an abortion ban in your state with no exceptions. Someone's *location* where abortion is outlawed is a **structural** domain of power and experience with an oppressive culture or work environments we think of as **cultural** and **interpersonal** power. For example, the boss who threatens your career and legal risk because they are anti-abortion might exert **cultural** and **interpersonal** power. Since it is possible based on location for the healthcare worker, friend, or relative to be the person who reports e.g., suspicious miscarriages, this might also fall under **disciplinary** power or **interpersonal** power. All of these matrixes of power interrelate. In our findings, when we discuss our intersectional risk populations, we refer back to Collins' framework.

None of our participants used the language "structural," "cultural," "disciplinary" or "interpersonal" rather they talked about perspectives and experiences that we relate to these constructs throughout the findings.

4.1 Laws, reproductive risk, and privilege

Most participants have an idea of whether abortion is legal in their state, and this is often given as a reason they do not have to worry about their technology use. In a sense, the domains of power that form Collin's matrix are not in play (abortion is legal) so participants don't feel the need to take major steps to protect their privacy. Even for many of those who are in states that are hostile to abortion (e.g., where changes in elected leaders might usher in changes to their state's constitution in ways the criminalize abortion) or where abortion is currently illegal (or thought to be), the strategy usually doesn't involve technology e.g., to have a plan for moving or going across state lines for an abortion. Being in a location where abortion is not banned seems to confer privilege that overrides individuals race or ethnic backgrounds. Where we later see experiences overriding privilege is when reproductive risk level comes into play and/or some combination of illegality and experience with oppressive states or interpersonal relationships.

Stephanie describes not being concerned because abortion is legal in her/their state but says that it would be worrisome if she/they lived in a state where it was illegal:

> "I mean, I'm fortunate. I live in a state that still allows it. So, I'm not as concerned. I mean, if I were in maybe Alabama or Texas I would be more concerned. So, I think it depends on what state you're in and then what age you are."

Stephanie who is in marketing in the technology sector describes having access to professional channels and friends who discuss technology strategies for reproductive privacy. Stephanie says that if she/they lived in a state where it was illegal to get an abortion she/they might take precautions like encrypted messaging and concealing her/their IP address to book appointments or travel related to reproductive health: "Yeah, I mean, I think if you're in a state that bans it you might have to use incognito

search on your Internet searches, maybe, so you can't be tracked if you try to register for appointments or maybe, if you need to book travel outside the State. Probably just have to protect your Internet privacy and your messaging, so probably need to use, um, Telegram or Signal for messaging services that don't track or keep record of your conversations."

Clearly, Stephanie views location as privilege to not engage with privacy precautions. Stephanie does not take these precautions her/themself because, as Stephanie points out, she/they lives in a state that does not ban abortion. It is not that Stephanie doesn't know what to do, rather location privilege shapes the decision to not bother with these measures.

With Victoria we see where privilege, in the form of state law, is considered a reason to feel safe with technology, but that nevertheless it seemed wise to delete her/their period tracking app. Victoria who is older with kids and not looking to get pregnant was disappointed to delete it because she/they says it was very useful postpartum. Victoria says that even if she/they felt safe in her/their state, it is still a good idea to avoid using a period tracking app:

> "Um! I had previously been using a period tracking app which was just really helpful, especially in the post-partum area when periods could be all over the place. I am feeling like, even though I'm in a state that's quote unquote safe right now, like I, I probably should avoid using that app, which is a bummer, because I really don't want to use a paper and pencil calendar um in terms of people."

Victoria goes on to describe learning that there are data privacy issues associated with period tracking apps and that companies are not always transparent about what they do with the data. There were also a lot of people on social media saying to delete it and some news media stories about how large companies were sharing data with authorities:

> "I did some research. It involved digital things I already knew. There's some data privacy issues, and not all companies are transparent about what they do with their data or who they give them to. Um, but also, I saw um just as a regular person on a lot of social media spaces people saying, 'delete your apps, those are going to be tracked and shared.' Um and it, you know you're starting to see some news stories, too, of large companies sharing some data with authorities."

In essence, Victoria is willing to take action on things that seem obvious (like deleting a period tracking app) but isn't going to take any other steps in terms of digital privacy. In fact, Victoria was hesitant to go too far with researching digital privacy post Roe because she/they has a "hectic life" and didn't need to add to her/their worries.

Throughout our interviews, no matter what participants race/ethnicity, being in a state where abortion is not banned confers privilege such that participants did not feel that they had to take steps with their technology or otherwise conceal their behavior. When laws seem to become less clear or where there are elections that threaten abortion bans, we see a heightened sense of vulnerability. This vulnerability doesn't necessarily mean that participants will take the measures that Stephanie suggests, only that they might consider their options (e.g., what to do with embryos, whether to move to another state). When

participants have additional added reproductive risk on top of experiences of risk with laws and culture, we see more dramatic steps being taken—making the argument for why this issue is intersectional. In the next section, we explore why technology intervention is not necessarily considered an option.

4.2 'The Handmaid's Tale' as an outlook and strategy of the privileged

A number of participants framed concerns about privacy in terms of a *Handmaid's Tale* scenario in which the data on their phone, or collected about them by medical institutions, on the "dark web," or by some "right-wing" activist organization could be used at any time to criminalize their behavior. Claims to *Handmaid's Tale* thinking are most prevalent among people who are older and feel less of a "target" for prosecutorial risk (i.e., do not feel the weight of **cultural** and **structural** domains of power) and may also have a low reproductive risk—not seeking to get pregnant or not likely to have a high-risk pregnancy (i.e., do not feel the weight associated with disciplinary and structural power)—possibly reading themselves into the dystopic storyline in which they are not vessels of reproduction because of their age. These women feel that literally and culturally they are not at high risk and in that way, eliminate another intersectional factor that might oppress them[9]. This type of thinking makes sense because it gives them the opportunity to claim knowledge of privacy risks associated with use of technology risks without allowing them to be entirely real—the *Handmaid's Tale* is, in the end, a fiction.

Victoria is not too worried about the consequences of technology use because she/they is in a "safe" state, in a stage of life that is not a "high scrutiny bubble," and because she/they is not actively seeking to get pregnant. That said, Victoria does consider what she/they describes as a *Handmaid's Tale* reality. For instance, Victoria wonders if she/they were to call her/their OB/GYN and ask to be seen immediately, would that raise red flags? For Victoria, *The Handmaid's Tale* is the sort of predictive algorithmic potential of the medical information she/they contributes to conversations with healthcare providers. Victoria *does* trust medical staff but notes that when leaving the hospital after having a second child, she/they wrote vasectomy on her/their record because they ask for method of birth control. It's not that this information is incriminating, it's how much information gets out and possibly never deleted. Victoria imagines that in a *Handmaid's Tale* situation when data from five or more years is fair game it doesn't matter who you trust. The idea is that well intentioned individuals could document things that in a "*Handmaid's Tale* situation" could put Victoria at risk:

> "Like, if there is a weird *Handmaid's Tale* situation, where, like, you know, data for the last five years is pulled, and they start making inferences based on certain data trends [recorded by healthcare workers]."

Victoria says that if this were two years ago, when she/they was at a higher reproductive risk and trying to get pregnant, she/they would be more worried about sharing information with medical professionals. Victoria didn't use IVF but considered it and wonders what would happen now if she/they used it. Victoria considers multiple scenarios like this that seem riskier in hindsight, working her/their way through risk assessments from then as if they were now.

[9] See Patricia Collins matrix of domination which includes hegemonic power (the ideas produced by dominant culture) [28].

Victoria is a clear example of where heightened reproductive risk might influence digital privacy management, even in a state where there is legal "privilege." Victoria's concerns also raise important questions about how well-intentioned care workers can essentially become the adversary. It also highlights how an understanding of how information is never forgotten (i.e., "data for the last years is pulled") might make any attempts at future reproductive privacy seemingly futile.

The *Handmaid's Tale* also came up for Elisa who did not feel she/they was a target living in a state where abortion was legal, in her/their 40s, and no longer seeking to get pregnant (i.e., low reproductive risk). When recollecting privacy technology choices in the days and months after Dobbs, Elisa recalls deciding *not* to sign a petition and would have deleted anything period-related on her/their phone, citing *The Handmaid's Tale* as justification for this thinking:

> "So, like there was a petition to like fight against it. And I didn't sign that just because I was like. 'I don't really want to put my name on anything because, I did watch the Handmaid's Tale.' Still, you know it's fiction. So, I did not remove anything from my phone (but I did hear that people were) because I didn't have anything really on my phone … with regard to my period."

Elisa decided not to engage in certain online activities that communicated her/their political stance and would have deleted a period tracking app if she/they had one, but was not planning on taking any other measures because of her/their perceived privilege (location, age, and reproductive risk).

Emily, who is young and has had children, feels relatively safe in her/their current state where there is no trigger law and there is an effort to put abortion on the ballot for state constitutional amendment. Yet Emily's experience living in a more repressive state influences her/their plans for travel and what technology she/they will use when crossing state lines. That is, Emily is an example where experience with oppressive states influence perception of risk.

Although Emily does not explicitly reference it, these are the types of things that are part of her/their *Handmaid's Tale* thinking: Emily deleted a tweet about the Dobbs decision, in retrospect because it seemed not in keeping with her/their account, which is professional, and also because of fears of ending up on some list of those being surveilled for future prosecutorial action. Emily also worries that her/their husband is from a state where abortion is not legal and where there are rumors of politicians or organizations (she/they are not sure) assembling lists of women who have had abortions. For this reason, Emily worries about crossing state lines and about GPS tracking. Emily also did call up her/their OB/GYN after Dobbs regarding her/their embryos—i.e., should abortion be outlawed, unwanted embryos might also be. Emily also worries that her/their medical records, even though they are supposed to be deidentified, are shared with the government for quality checks. Emily considers that online shopping could put someone at risk but is less worried about that because of her/their modest online shopping habits. Despite Emily's assertion that her/their online shopping habits are modest enough not to be a concern, she/they acknowledges that virtually any shopping online or with credit cards linked to reproductive health could result in someone learning they were pregnant.

> "Oh, gosh! I mean, I guess like things like Amazon, I mean if you have like an Amazon subscription for like pads or tampons, and then you stop it, I guess, or even like, you know, I've heard some of my friends when they got pregnant like, somehow, they will get like formula sent to their house, or something like [that]. I haven't had that happen to me personally. Um, but I've heard of that happening, so I guess credit cards, or, like Amazon subscriptions, would be like another thing … I'm not someone that like has a bunch of subscription services, or like, had a subscriptions to like daily products."

While Emily's location confers privilege, the experience of growing up in, and traveling to (currently) repressive states compounded with reproductive risk make her/them more cautious traveling to another state, where GPS tracking might be a concern. Emily is aware of the structural risks because of experience with cultural or interpersonal power.

Lily, who is mixed race and prefers to self-describe her/their sexual orientation has had experience with abortion under circumstances following rape and other accompanying trauma. Lily still mourns the child she/they lost but also knows it was the right decision for her/their education and career. Lily is an activist for human rights and, like several of our participants, has a passion for reproductive education. At 40, Lily is trying to conceive and facing new medical complications that make an ectopic pregnancy an increased possibility. Lily decided not to download a period tracking app after hearing on NPR that it was not safe. Lily also heard that IP tracking was a concern and would consider that if she/they had to look for abortion clinic. Otherwise, Lily hasn't considered anything else saying that we live in a *Handmaid's Tale* reality (which she/they equates with Gestapo and Nazi Germany) currently and she/they essentially feels helpless:

> "No, it's just. I was like. Are we really gonna get to that point where it's kind of like the Gestapo like in Nazi, Germany like where you can … I never watched the *Handmaid's Tale* to be honest because … It actually could happen. And that's why I've never watched it because it's real life … I know what the gist of the show is, just because everybody posts about it. But it's almost like we're already there like that. They're going to be able to just access. And if they pass these laws that you know where they can criminalize you, they're going to have the FBI or CIA anybody investigating. You can have your search results from your computer."

Like the other participants in this category, Lily envisions a *Handmaids Tale* reality in which lists are being created and IP addresses are being tracked. Lily also worries for young generation who are of a more fertile age and might not be ready. Lily speaks of "generational trauma" and that her/their mother didn't want to be a mom and about abuse in her/their household before saying, "It's cruel to not have the choice, because it's a decision between you and your doctor." But for Lily, perceptions of risk are narrowly constructed around changes to the legal climate and medical circumstances. Lily has several factors (location, reproductive risk, and past experiences with trauma) that might make her/them more cautious. But Lily's outlook is shaped by a sense of helplessness ("They're always tracking us") and the knowledge that the laws in her/their State do allow for abortions in certain medical circumstances that would apply. Although among the strictest in the country, her state does make exceptions for the life of the mother (and in cases of incest and rape), which she/they finds reassuring.

Not all participants explicitly talk about a *Handmaid's Tale* but maintain a nihilistic view that they are always being tracked and that they can't do anything about it and/or don't want to live their life worrying about it constantly.

Kim who is trying to get pregnant with in vitro fertilization (IVF) and has, in fact, increased her/their use of social media to keep tabs on the laws regarding embryos says that, "I feel like Facebook and Google are always listening to us, and I feel like everything we are discussing because I have the Google Assistant in my house and every room, and I feel like you know anything that we discuss in the house or share online or communicate online. All these different corporations are collecting all those information, and I don't know how they're being used … I mean there's only so much I can do, because you can only protect yourself so much. I can't be like really, picky, so I mean right now it just. I can [accept being tracked]." While Kim is privileged in terms of her/their location she does have reproductive risks. Kim seems to be aware of her/their resignation and it seems to play a big role in her/their lack of concern for privacy management strategies.

Veronica provides a case of someone whose higher reproductive risk does lead to concerns about privacy but a sense of helplessness or apathy in terms of technology surveillance results in her/their not taking any digital privacy management strategies. Veronica is seeking to get pregnant and is at a higher risk of miscarriage. Veronica does worry about the repercussion of sharing her/their fertility journey with people because she/they doesn't want to be judged. But knowledge of this **cultural** or **interpersonal** power does not extend to concerns about prosecutorial repercussions despite some concern about laws. When it comes to technology, Veronica says that even though she/they had friends who worry, it isn't going to change anything: "To tell you the truth, you know I don't know, but like. They are for sure for sure. So, some things they just they don't really like to talk around their phones. They turn them, like, if they having deep conversations, they will turn their phones off … But I kind of, I don't want to live like that, you know?" Veronica is not positive that there is near total surveillance of her/their phones as friends suggest but is also not willing to make drastic changes in order to guard against it.

4.2.1 Age & stage of life

As we have discussed, location/laws confer privilege, as does being older and not seeking to get pregnant, which essentially equates to lower reproductive risk. We also mentioned a sense that, culturally, being older is perceived to put someone at lower risk; that is, they are not a "target" for vigilante-enforced bans or prosecution.

Stephanie and Elisa provide an understanding of how participants are thinking about their reproductive risk in terms of their age and family planning:

> Stephanie who is not sexually active and not looking to have children believes she/they is at lower risk: "At this point, I'm toward the end, because I'm 43."
> Elisa is firm in the belief that she/they is not at risk, "No, because I'm forty, and I have one child, and I don't plan on having any other children."

In the next section, we will look at where lack of privilege in the form of youth (**cultural** domain of power), reproductive risk (**disciplinary** and **structural** domains of power) and experience with oppressive states or environments (**cultural** and **interpersonal** domains of power) trumps location privilege.

4.3 Young (cultural domains of power) /high reproductive risk (disciplinary/structural domains of power) and practicing no/low-tech strategies of the less privileged

Those who are younger and sexually active tend to be preoccupied with no/low-tech technology privacy strategies like good contraception and being choosier about partners, and for these reasons feel safe. Being younger equates with higher suspicion **(cultural** domains of power) and higher reproductive risk **(disciplinary** and **structural** domains of power)—not only because they may be more likely to get pregnant but because several cannot or chose not to be on birth control. There are some younger participants for whom risk of high-risk pregnancy outcomes also impose **disciplinary** and **structural** power because abortions (if there are complications, genetic issues, etc.) or embryo disposal (i.e., for those who struggle to get pregnant) may be outlawed.

A few participants like Rowan stressed being attuned to their bodies as a way of dealing with these power differentials:

> Rowan is a bisexual, multi-racial woman who is very concerned with reproductive health education. Rowan says that abstinence and safe sex are first defense against changing laws about abortion. Rowan says that she/they has been feeling this way for a while, but that Dobbs "solidified" that resolve to be more conscientious about sex—choosy about partners and more aware of her/their body. In the event that Rowan did get pregnant (and Rowan really expects that will not happen), she/they would go to a planned parenthood.
>
> > "To be honest, I just. I feel like I'm in the position where I just rather … be as cautious as possible to not have you put in that predicament. But if matters do arise. Well, I know what to do with that situation."

Rowan did delete her/their period tracking app but is primarily focused on how to prevent unwanted pregnancy with her/their philosophy of choosing partners and having conversations with them upfront—which Rowan attributes, in part, to her/their race and sexual identity. Roman also has the added concern of not wanting to go on medication birth control, so conversations about other forms of birth control are necessarily consensual.

> "I'm bisexual so like that's kind of like from the get-go. So, I kind of can like gauge … if they don't like LGBT people, they're probably …. it's further than just like talking or like engaging with someone like from like the get-go. But I would say, um, in terms of the conversation about like reproductive health. Kind of talking about, 'Hey, like, I want to use condoms, and I do not want to get pregnant. I don't want kids. I'm sure you don't want kids right now, at least not with me.' And kind of just be able to have this conversation, because the fact of the matter is, I'm not going to go on birth control, because I don't want to, for my personal reasons. Um. So you're going to use a condom if you're going to have sex, and if not, then I guess you won't be having sex and like that's really as simple as it gets, because I'm not going to compromise that me personally."

Rowan's age (**cultural** power) as well as reproductive risk (not being on birth control) and to a lesser extent race/identity shape her/their reproductive privacy strategy. Rowan manages these **cultural, disciplinary,** and **structural** domains of power with abstinence, better cycle management, and partner selection—i.e., non-tech strategies.

Other young participants acknowledge the risks of reproductive data while at the same time, pointing out that people should also just be careful about their sexual practices. For instance, Antonia considers that browsing histories and online tracking might be a concern but prioritizes what she/they can control, which is her/their body—and tends to adopt no/low-tech strategies. Antonia also has had some bad experiences with healthcare facilities (including in the context of abortion) and would rather avoid trusting anyone when it comes to advice about reproductive privacy decisions. Antonia recounts a harrowing experience with healthcare workers during an abortion in which they seemed unresponsive to her/their medical needs and unwilling to provide even a minimum of information including the side effects of abortion medication.

> "I don't know if I should be careful about browsing and incognito tabs and being worried about like, my data tracking, because I know it's getting crazy … We really need to be in control of our own bodies, and that's just me, I guess I'm untrusting, because I've never had a doctor who I've had a trusting relationship with ever so it's been me on my own."

Antonia, like a few of those we interviewed, is not familiar with the law (**disciplinary** and **structural** power) in her/their current state but would figure it out should something happen. Antonia feels that being from New York (where her/their family is based) means that she/they is safe because it is still legal ("for now"). Interestingly, Antonia perceives that she/they is "privileged" by her/their location, even while her/their inability to be on birth control put her/them at even higher reproductive risk.

> "Okay. So me, I'm privileged. I'm lucky I'm from New York. So if I had to go back home, or if I had to get something to delivered somewhere, I'm safe in New York for now, for now that's just for now."

That said, as a bisexual individual, Antonia describes being conversant in the "coded" language that she/they and other marginalized friends have used to keep themselves out of "Facebook Jail"—a timeout that Antonia has experienced when Facebook suspends accounts for violating community standards. Antonia talks about how experience (particularly with friends that are BIPOC) have given her/them insight into and practice with coded language (e.g., using "wheat" for "white," or a symbol of wheat so you don't get flagged for saying "white nationalists" etc., terms that Facebook has banned). Antonia believes she/they knows well how to use "coding" to get around algorithm/surveillance and thus navigate an abortion through online channels if necessary. When asked, Antonia mentions coded language used to locate people who will help with abortions in other countries.

> "I also have a large community of people online who kind of have, like an underground railroad system going, if you need to come somewhere if you need [code word for abortion]

Antonia who is young and not on birth control and does not trust healthcare institutions manages **disciplinary** and **structural** as well as **cultural** and **interpersonal** domains of power through

reproductive education, off-line cycle regulation, and a digital strategy involving **low-tech coded communication**—a kind of subversive cultural power. In a certain sense, Antonia represents the kind of no/low tech "literacy" that is required to navigate a multi-vectored and highly contextual set of risks.

Several of the younger people whom we spoke with cannot be on birth control for health reasons.

One in particular, Rocky, feels quite frightened. In fact, Rocky and her/their husband moved from a country where abortion is illegal to the US in the hope that it would be better for them. This person discussed considering whether to relocate to another state because theirs was currently hostile to abortion rights. Rocky has always been cautious about using Google but is now more so since the Dobbs decision. At the same time, Rocky perceives that she/they will be safer if she/they moves to a state where the right to abortion is guaranteed by law saying that "I will be more comfortable at least sharing my decisions online, or getting back to using Flow [the period tracking app]. Because I know whatever happens law would support me."

Rocky has a high reproductive risk because of the fact that she is young (**cultural** domain of power) and cannot be on birth control (**disciplinary** and **structural** domains of power), has experience living in a repressive country (**cultural** and **interpersonal** domains of power), and is in a location where abortion is under threat (**structural** domain of power). Rocky considers mostly non-technical solutions—i.e., moving to another state, not using Google search. Rocky also manages power differentials with the prospect of regaining structural power by moving to another other states.

4.4 Reproductive risk (disciplinary and structural)/experience risk (cultural and interpersonal domains of power) and more tech savvy strategies of the less privileged

We found that participants who have experienced **disciplinary/structural** or **cultural/interpersonal** risk were more prone to take steps to secure their privacy and to do so in a way that combined high and low-tech approaches. Sylvia is young (**cultural** domain of power), has experience with repressive environments (**cultural** and **interpersonal** domains of power)—including living in a state that bans all abortion (**structural** domain of power) and has seen how pro-choice stance can threaten job opportunities. Jessie is pregnant, in a state that bans abortion, and has high reproductive risk (**disciplinary** and **structural** domains of power). Both employ more sophisticated technical strategies for the sake of their reproductive privacy, Sylvia primarily because of past experiences with social/job risk (**cultural** and **interpersonal** domains of power) and Jessie because of her/their reproductive risk (**disciplinary** and **structural** domains of power). Neither one feels they are targets per se but worry more about the complex nature of surveillance offline and online.

Sylvia worries about the repercussions of sharing information with people in her/their personal and work life who might not agree (**cultural** and **interpersonal** domains of power). She/they have experiences with discrimination in the past and worries her/their views could have negative implications on her/their career. Sylvia doesn't think she/they is on the "radar" of the government or pro-life activist "vigilante group" necessarily, but considers that there could be implications from her/their data (e.g., private conversations on social media, search history, etc.) being used in nefarious ways by people seeking

to prosecute or even protest outside clinics. Sylvia explains that the data used by marketers to profile consumers could also be used to target someone and then hack into their personal data. Sylvia has also had friends who have written privately about their pregnancy complications and then received hate mail; in her/their view the privacy of social networks has "been compromised." Sylvia makes connections between online behavior and violence friends have experienced outside clinics, noting that she/they doesn't think online behavior was the vector but that it could be. In Sylvia's view, the biggest concern would be if somehow her/their online data were used for personal attacks, which Sylvia doesn't believe is that likely, given that she/they is not a public figure:

> "I guess there's a couple of possible scenarios. One is like a larger company, say Google or Facebook. These companies that have access to so much data, using my data points among the conglomerate of millions of other people for me. That's less of a concern. The bigger one would be like a personal attack. And realistically, I don't think that I'm kind of visible in the public sphere enough to be at risk for this, or to be at a large risk … whether someone's hacking your computer, whether they're installing some sort of monitoring software. I think that the effort required to do that … would be much more likely to be applied to someone like a public figure, a politician. I don't know a well-known actor or actress whatever, so. I don't see myself as the main target of this. But I'm just, as I say, I want to take every precaution possible, especially since, in my case, the cost of taking a precaution is relatively minimal; and though I don't see this as a directly pertinent risk, I think the consequences should it happen should someone be tracking me? Um could potentially be very severe, and I would love to avoid that, if possible."

Sylvia is primarily worried about people finding out about her/their abortion stance. The precautions that Sylvia is taking, to essentially avoid **cultural** and **interpersonal** domains of power, include **low and high-tech strategies** like being more careful about what she/they says online and using a VPN. This "minimal" effort Sylvia believes is worthwhile given the severe consequences, which to her/them are vivid: "In this case. I see this more as a hypothetical, but I definitely think that sort of big brother scenario, be it a government agency, or some sort of vigilante group in terms of monitoring individual data is a possibility. And so again, I see this as more a bit more removed from my particular scenario. But um! That scares me and um I've heard of just so many stories about people going to clinics and being, I even know someone who went and was like followed … like some larger group or organization tracking my day."

Jessie, who is currently pregnant and queer, was aware that her/their medical condition put her/their at an increased risk for miscarriage (**disciplinary** and **structural** domains of power) or the need for abortion. In Jessie's case, she/they is in a state where abortions, even for ectopic pregnancies, are illegal (**structural** domain of power) and so had a plan for how to get it done in another state. The plan involved VPNs, cash, and other legal considerations. Jessie is thus cautious, but also felt that she/they wasn't the target of investigations because she/they felt that poor women who do not have people to advocate for them are the primary targets: "The women that have been prosecuted for miscarriages and things like that have been poor and unable to advocate for themselves. They are easy targets. The worst that happens is, we have to leave the state." Jessie is taking precautions with VPN, with browsing, but does not anticipate prosecution. At worst, Jessie would have to leave the state.

There was, however, one participant for whom location alone (**structural** domains of power) was a motivator for **low- and high-tech strategies**. Lucy's perception that abortion is not legal (though it is in her/their state) has made Lucy more careful about sharing online. Even before the Dobbs decision Lucy was careful about use of social media. Lucy turned off google tracking whenever she/they "remembered" and wasn't using it for navigation. Lucy is also careful about passwords. Lucy says that she/they takes the precautions because of "bad stories" she/they has heard about friends being scammed. If Lucy were to have an unwanted pregnancy it would mean going to another country. Lucy also mentions that, while very careful, the overturn of Roe v Wade might compel her/them to use double contraception.

5 DISCUSSION

The participants we spoke with are not empowered to do much but conceal, with great effort, the things that they do; and when they are under no imminent risk (e.g., because of their reproductive risk or where they live (**disciplinary** and **structural** domains of power)) or have not experiences with repressive environments (**cultural** and **interpersonal** domains of power) they will not alter the technology they use outside of erasing their period tracking apps.

The media has portrayed period tracking apps as a (or *the*) major risk factor for reproductive privacy in the post Roe environment [102] and, as consequence, participants seem to believe this is their only official method of agency—even if it is, perhaps, performative because they recognize the futility. They do perceive that reproductive privacy could herald a *Handmaid's Tale* reality but can't do anything about it, and their privilege also justifies not taking steps to change their digital privacy management. But as our findings suggest, lack of agency can result in different outcomes depending on the perception of risk and other contextual (power-related) factors:

Some participants who are more vulnerable because of high reproductive risk (**disciplinary** and **structural** domains of power), location/law banning abortion (**structural** domains of power) or experience with oppressive states or environments (**cultural** and **interpersonal** domains of power) are seemingly more concerned about privacy and equipped to navigate risk **either with high technology strategies or no/low-tech strategies, or some combination**. By contrast, our younger population (**cultural** domains of power) more attuned to using strategies that were no/low-tech.

Privacy researchers should explore how these individuals navigate this space and how they employ technology strategies. In the following section, we discuss the implications for intersectional analysis, elaborate on findings' implications for the media and privacy theory and research, and conclude our discussion with some guidance for researchers using the intersectional privacy intermediary lens.

A note about surveillance and its important role in privacy research. The certain specific characteristics that we found to be relevant in deciding privacy strategies having to do with reproductive risk, laws, location, and experience with oppression all have to do with surveillance, be it medical, social, or legal, suggesting that surveillance theory is an important lens to consider when exploring how power influences privacy strategies [65]. For example, Kim, although an immigrant minority, did not feel her/themself to be at that much risk because the lack of clear and present **structural** and **disciplinary** power and so decided not to do anything, even while acknowledging the feeling that she/they was always being surveilled. By

contrast, others who felt **cultural** and **structural** power more acutely, took steps to sidestep surveillance with a combination of high and no/low-tech strategies.

5.1 Using an intersectional interpretative lens in HCI

In our results we describe how certain overlapping categories (age/reproductive risk, location/laws, and experience with oppressive states or environments) shape privacy strategies and the ways those map to Collin's matrix of power. Living in states where there is no abortion ban and having low reproductive risk (i.e., lack of experience with powerful domains) equates with a *Handmaid's Tale* way of thinking about privacy management which is, we argue, privileged. By contrast, being young and/or of higher reproductive risk (e.g., fertility issues, sexual activity, inability to use contraception, risk for miscarriage, ectopic pregnancy or genetic conditions, etc.), living in states that ban abortion, and/or experience with oppressive states or environments (e.g., trauma, distrust of medical professionals, workplace discrimination, etc.) all fall along one or several axis on Collin's matrix and lead to no/low-technical or more technical strategies, or some combination. It is evident that these strategies may equate with type of risk. For example, younger participants seemed to be more invested in old fashion period tracking, selective partnering, and abstinence (all no-tech strategies) than their older counterparts.

Those who did not live in a state where abortion was banned and who were not at high reproductive risk had an outlook consistent with what Collins conceives of as hegemonic or **cultural** power under which matrix of domination take hold. These participants perceived that we live in a kind of *Handmaid's Tale* world where reproductive freedoms are no longer guaranteed**.** But, for now, they depend on Collins' **structural** power (how laws and policies are implemented) to maintain their status as "safe." **Future research should explore the extent to which concern about structural power (e.g., law enforcement) translates to technology behavior. Perhaps to better understand privacy strategies and perceptions, HCI researchers should explore these metaphors about power through elicitation.**

By contrast, those who were younger and oppressed by **cultural** power were more likely to rely on privacy strategies that avoided technology altogether, perhaps because of their perceived visibility as being of reproductive age. Fear of **cultural** power may be an important construct determining privacy strategy, and one that is related more to social surveillance, where the vectors of threat are more ambiguous and perhaps, more low tech. Those who perceived themselves to be at high reproductive risk (**disciplinary** and **structural** domains of power) or living in a state that banned abortion (**structural** domain of power) were more likely to take a combined high and low-tech approach, perhaps because of their privilege and perceived *lack of* visibility, which, for example, Sylvia emphasized. They also may have felt their threat had more technical advantage. **HCI researchers should be attuned to these complex and shifting power matrices that influence changes to perceptions, use, and receptivity to privacy strategies.**

By framing our study around intersectional relationships of power, we were able to look at a less typical interrelated axes of power involving reproductive risk, location/laws, culture and personal experience. **Finally, HCI researchers should approach studies of technology use and privacy risk by first exploring the way that identity facets and intersectional characteristics influence perception of risk and mitigation strategies with technology, and, in particular, be attuned to strategies that do not involve technology.**

5.2 Examining the media and argument for using a more critical lens in HCI

It should give privacy researchers pause that media emphasis on the risks of period tracking apps was apparently so effective that all of our participants erased them from their phones. As noted, period tracking apps, while notoriously insecure, are essentially no less harmful from a tracking and data triangulation standpoint than other apps people download to their phone. While period tracking apps are selling period data, many other pieces of data can be used to detect reproductive health status, including search and location data and purchases (e.g., menstrual pads). Perhaps providing insight into these practices and basic guidance about obfuscation [22] could go a long way. **HCI researchers should be critical of how technology privacy is portrayed in the media and its potential for shaping norms that they in turn study (e.g., [69]).**

It may be too late, as some participants acknowledged, to take back medical health histories that put them on "abortion lists," but understanding (or being reminded) of what medical histories reveal could support small changes to behavior. Obviously, there are tradeoffs between providing accurate personal health data (for example, like contraceptive methods as one participant pointed out) and protecting one's privacy.

Overriding this is the media's lack of attention to privacy's intersectional risks. Our study only begins to scratch the surface, but it is clear that when it comes to privacy no one size fits all. Individuals need help sifting through what are reasonable reactions to legitimate threats, and those differ depending on the person and circumstances. The response from the media was an urgent message encouraging *all* women to delete their pregnancy app, followed by a set of articles saying this was not nearly enough. A better approach might have been to provide information about vectors like application location tracking, browsing history, unencrypted messaging and so on and then provide adversarial strategies like reporting to authorities that result in warrants, organizations that pay for third-party data, and others so that people could decide where their vulnerabilities are and what to do about it—be it turn of their location tracking, leave their phone at home, or be careful about who they talk to. In some sense, consideration for different domains of power would be helpful. For instance, consideration of vectors of threats from health care workers that are suspicious of miscarriage (**disciplinary** domains of power) or being wary because of currently or in the past living in environment in which abortion is looked down upon (**cultural** domains of power) that could leave someone more susceptible to reporting or simply an understanding of the laws and what they ban and when (**structural** domains of power). These are no fail-safe measures but we should inform the public in a way that helps them think intersectionally and contextually about their risk, and thus allow them to manage it.

Based on our research alone, media should focus on guidance that is geared towards legal climates and reproductive risk. The media could frame information that would support privacy decisions around state laws and reproductive risks. For instance, individuals should be aware that IVF puts them at an increased risk for ectopic pregnancy, which puts the pregnant person at risk for death and some states do not have exceptions for terminating ectopic pregnancies. This was a deciding factor for Lily. **HCI researchers need to be attuned to media narratives and missteps and consider how that might influence their research design, or provide avenues for critical research.**

5.3 The implications for HCI privacy thinking and framing

5.3.1 What the privacy paradox and literacy efforts get wrong

Media discourse arguably has a huge influence in determining what is normative and what individuals' expectations of privacy should be [69]. In the wake of the Dobbs decision, why weren't privacy researchers sounding the alarms about other (more serious) threats? This may, in part, be because privacy research has been preoccupied with what users don't know about their privacy and how to generally nudge them into better habits—overcoming the so-called privacy paradox, without regards for contextual risks that govern these decisions [91]. Privacy research has, understandably, focused on how users behave in a given context—on a platform—typically with the goal of understanding how users engage, as indices of user sensitivity and vulnerability.

Given that most of those who may become pregnant have, only within the last few months, occupied privileged positions it seems reasonable that they may only be willing to delete period apps. What works necessarily depends on perceptions of power (institutional/**structural** and **disciplinary**, social/**cultural** and **interpersonal**, and legal/**structural** factors), identity, and context.

With the exception of those who face high risk, participants' lack of urgency to do anything beyond delete period tracker is notable. But it can also be true that, as our findings suggest, individuals are deeply aware of the fact that they are always being tracked and feel helpless or resigned [36,55]. Many participants describe the way ad algorithms pick up on the things they do and say as evidence that they cannot escape their data being tracked. The *Handmaid's Tale* reality is ostensible an authoritarian one, or, at very least, a right-wing extremist one. It's also still, by and large, a hypothetical one, something they can imagine, but not practically act on. There may also be an extent to which this is a result of individuals' feelings about privacy (or optimism) aligning with the political party currently in power, which is against criminalizing abortion [50]. If power shifts in congress, and a nationwide abortion ban is approved, we might see different behavior.

For those that do face high risk, we need to better understand how to support them, without providing pedantic and misapplied "literacy" to a problem that is highly nuanced and contextual as our participants demonstrated. For example, it is possible that one of the best strategies for some might be to learn how to track their cycle with a pad and paper. It's also possible that they also might need to buy period pads in bulk so that changes in their patterns are not detected. As mentioned above, education about risks need not only be about technology risks but about, in this case, reproductive risks. There are any number of things that aren't necessarily technological that could be helpful but there are certainly also things that people who are at high risk should not do. Privacy intermediation (which we discuss in 5.4) must be about thinking in this intersectional and holistic way.

5.3.2 No/low-tech strategies

We identify the no/low-tech strategies used by some younger and/or higher reproductive health risk participants: younger participants (**cultural** domains of power) often described **no/low-tech** methods for

avoiding abortion (e.g., contraception, abstinence, body awareness, good judgement, etc.); those facing higher reproductive risk (**disciplinary** and **structural** domains of power) or in states with an abortion ban or experience of oppressive laws or social outlooks (**cultural** and **interpersonal** domains of power) were also more concerned but may have been using more **sophisticated technology strategies in combination with no/low-tech strategies** (e.g., traveling, avoid bringing phones with them and/or not searching on the internet for clinics). It is instructive to consider that no/low-tech strategies is not a new phenomena [66,71,98,101], and a reminder that "digital privacy literacy" efforts may not be entirely what are needed. In fact, the "literacy" that participants often drew on to ward of threats to their privacy was health education related and familiarity with local and national laws, rather than technology literacy. Notably, those who are experiencing **cultural** domains of power may be those who are most likely to **not use technology** since their status as young and of a reproductive age is harder to hide. It gives us new insight into the impact of **cultural** power (which tends to equate with social surveillance) vs **structural** power (which tends to equate with government surveillance) on privacy strategies. In terms of surveillance literature, we know that marginalized communities have been forced to take steps to protect themselves, and those tactics may be instructive as we look to mitigate risk more broadly [66,101]. For example, historically marginalized individuals are more often subject to discriminatory profiling and surveillance through—e.g., everyday law enforcement [41,42], foreign travel [35], immigration [18], social benefits [39], sex work [12,112], and throughout history—provide important insight into how to avoid threats using no/low-tech strategies. Surveillance of these groups can be difficult to escape and so the strategies may be uniquely honed [51]. Those who experience intimate partner violence (IPV) are faced with unique challenges because their adversaries are often able to infiltrate victims devices using low-tech strategies that defy technology threat models [47,95]. In that sense, these communities are evidence that privacy paradoxes (and digital literacy) are more reflective of structural oppression and norms, not actual skills [68]. Our research suggests the nature of oppressions and power can influence privacy strategies in ways that similarly do not have to do with "technology literacy" but literacy related to society, law, and health. We talk about literacy more in our guidance.

5.4 Guidance for HCI studies of privacy: through a privacy intermediary lens

The issue for studies in HCI and related privacy fields is then, whether and how we begin to study privacy in terms of the things that people do that do not always involve technology and how they perceive power structures, and their place in the world of consequences.

While, as HCI privacy researchers, we are not privacy intermediaries—that is, we are not those providing health, counseling, and other services to people who may become pregnant—this orientation can be used as a lens to think about how we do research, and also how we do so in a way that supports privacy intermediaries. That is, privacy intermediaries is both a concept and frame—a way of thinking about and orientation toward privacy research— and a role performed by those who provide privacy management guidance.

Below is our guidance on how privacy scholars might conduct research. These guidelines are drawn from findings from this research as well as the concept and role of privacy intermediation [71]. While we

seek specifically to including privacy intermediaries in research, we also intend for this set of guidelines to move researchers to think differently about their research:

- **First, we urge researchers to** identify and include **privacy intermediaries** in research. These could be service providers that people depend on for guidance, in this instance, health care workers, social workers, etc. **Rationale:** McDonald et al. [71] has highlighted the role that privacy intermediaries can play in development of privacy strategies for marginalized communities and for helping researchers to think about the intersectional facets of those they seek to study but which they cannot necessarily access. McDonald et al. and our research demonstrates the critical importance of discovery of these facets and the need to include those with sightline into these complex facets in research about populations at risk. Research with privacy intermediaries has the potential enhance the following guidance:
- **Guidance:** Researchers should have an appreciation for the risks and strategies employed by individuals whose surveillance has consequences not readily experienced by the mainstream. **Rationale:** We have shown that surveillance risk is important to understanding privacy strategies. Historically marginalized individuals provide insight into surveillance risks because they experience them more (e.g., [18,21,38,39,41,42,84,86]) and when they do experience them the consequences are graver.
- **Guidance:** Be willing to contend with fluid categories and think about privacy risk intersectionally, as a stack that is person-dependent. **Rationale:** We found that, much like Collins' work [28] advocates, this issue of privacy management was highly contextual and based on categories of risk that were not strictly race/ethnicity based (a common understanding of intersectionality) but on other dimensions of identity and experience that are somewhat more difficult to map but are still important [29,33]. (See more on the role of race/ethnicity in the next section).
- **Guidance:** Think of "technology literacy" as something that both requires other "literacy" and is so context-dependent that it is perhaps not useful as a framework for thinking about privacy management (including identifying its deficits). **Rationale:** For example, as we found, knowledge about reproductive risk was perhaps more important than understanding technological risk. Moreover, and somewhat relatedly, some of the strategies employed by participants were not (or seemingly not) technologically advanced like managing one's cycle, using coded language (echoing previous research [14,34]), or using birth control, suggesting that traditional notions of "technology literacy" are simply not useful. In some cases, participants felt that reproductive knowledge and offline behavior was more critical to securing their privacy, suggesting that concepts of "literacy" need to be profoundly broadened, if not rethought. Even if we don't abandon "literacy" as a concept, we still need to explore how to provide people with feasible strategies and a level of privacy "literacy" that goes beyond a tool-centered education. We need to consider the many facets of privacy protection that are necessary to achieve a more holistic proficiency over reproductive privacy, given the numerous and highly varied threat vectors to which menstruating people are exposed.
- **Guidance**: Embrace no/low-tech strategies as legitimate (maybe sometimes, the only) option. Rationale: We learned from younger participants, in particular, that no/low-tech strategies (e.g., like partner discretion and condoms) felt like the best option for them. This echoes previous research that has shown that no/low technology strategies and digital abstinence are sometimes adopted by "at risk" and marginalized individuals who might avoid digital record-keeping, rather than look for ways to safeguard

their digital records or engage in digital abstinence [43,71,98,101]. These strategies have been discovered to include "privacy intermediaries" who offer unique sightline into intersectional challenges face by marginalized communities [71]. For HCI researchers to embrace no/low-tech strategies, they must consider "literacy" and "agency" beyond technology, and conceive of users in a more holistic and intersectional sense. For example, does doing this type of research require a deeper understanding of people's reproductive health knowledge—as Kumar et al. discover [63]?

- **Guidance**: Model good privacy behavior. Rationale: It was really important that we were strict about participants obscuring their names and photos in video and having a limited conversation with us online, etc. These behaviors are important to normalize when doing research. It also keeps researchers from being vectors of privacy risk, and forces us to think about how we could ourselves be adversaries, guidance that is drawn from study of privacy intermediaries in other settings where they are well aware of their potential role as vectors of threat [71].
- **Guidance**: Explore metaphors that could translate/bridge to conceptualizing more favorable policy concepts like those outlined by the Electronic Frontier Foundation (EFF) [72]. Rationale: Many participants offered up The Handmaid's tale as a way of thinking about surveillance capitalism and authoritarianism. Indeed, we had participants summing up vast surveillance infrastructure with examples like, "you know when you see sweatshirt ads." Future research might explore how these concerns line up with policies that are being recommended in government or by advocacy organizations.
- **Guidance:** Be wary of assuming that, as privacy researchers and experts, we have any perspective on the "right" way. **Rationale:** We came into this research thinking or hoping that participants who were at risk for unwanted pregnancies would say that they were using specific privacy technologies and had to accept that better use of birth control was a reasonable low-tech solution.

6 CONCLUSIONS

We looked at the privacy strategies of those in the US who may get pregnant following the removal of constitutional protections for the right to have an abortion (i.e., the overturning of Roe vs Wade) and found that little had changed. What was in evidence was the success of trending advice about deleting period tracking apps, but not the millions of other apps that can pose nearly or as much risk to reproductive privacy. Also apparent was the deeply held knowledge of privileged individuals about this reality but little action on their part. At the same time, we identified a subset of participants for whom a set of overlapping identities and circumstances—high reproductive risk, age, location/law banning abortion, and experience with oppressive states or environments led to mix no/low- and high-technology strategy. These participants revelations about their reproductive privacy risk depended on their knowledge of reproductive risk, state law, and cultural risk and didn't necessarily align with "technology literacy." For example, we found that for those with high reproductive risk (**disciplinary** and **structural** domains of power) who lived in locations where abortion was banned (**structural** domains of power) or had prior experience with oppressive states or environments (**cultural** and **interpersonal** domains of power) the strategies were more elaborate and also included both high (using a VPN) and low tech (not using or bringing devices to reproductive related activities) approaches. For those who were younger (**cultural** domains of power) strategies tended to involve sexual abstinence and norm setting (e.g., putting partners through test of values), being in tune with reproductive cycles (rather than relying on technology to track

it) and being fluent in coded language that allowed one to find resources when abortion plans needed to be made.

Notably, reproductive risk, age, location/law, and experience with oppressive states/environments seemed to override race/ethnicity in in determining participants' strategies. This is not to say that race/ethnicity doesn't matter or plays no role in perceptions of risk and privacy management; indeed, we know that black women have a higher reproductive risk and carceral risk in the US [52]. Rather, in our research, we see that other characteristics, contexts, and categories of risk are also relevant. We expect that broader research would identify race as a factor. Although the core texts we draw on [28,29] argue this very point (that intersectionality is changing, complex, and requires examination of power and context), this understanding of intersectionality seems to be less surfaced in HCI scholarship. HCI has for several years been engaging with intersectional frames (e.g., [6,46,62,83,93,104]); but we argue that we need to continue to evolve that lens. As we have shown, this powerful lens has allowed us to identify various attributes that relate to age, risk, and geography, categories that are not (only) based on race. While more work is needed to explore the nature of intersectional risk in this space, we have identified important characteristics shaping reproductive privacy management which have implications for how we frame and study privacy in this realm.

6.1 Limitations and positionality

While we sought a diverse sample in terms of age, race/ethnicity, and gender and sexual identity, and location, we struggled somewhat to find younger participants. This could have been because younger participants feel themselves to be at greater risk and thus did not want to speak with us. While we invited anyone who may become pregnant to take our screener survey, but ultimately only interviewed cisgender women. Future work should include more diversity with respect to gender identity as well as sexuality. While we found that race/ethnicity was not a driver of privacy strategies (rather it was reproductive risk, age, location/laws banning abortion and experience with oppressive states/environments) it is very possible with a larger sample of people of color that we would have found that to play a role as well. Indeed, we know that reproductive health of poor black women is disproportionally policed and surveilled in the US [20,52]. Yet, we believe that the characteristics we identified are important to make visible.

We sought a diversity of participants based on race/ethnicity, sexuality, income, as well as locations with a range of different abortion laws. We were able to get a fairly diverse demographic sample but future research should seek a more distributed and diverse sample in terms of age, race/ethnicity, gender identity, sexual orientation, income, and location. Although we attempted to recruit from states where abortion laws are among the strictest, we were only able to recruit two participants from states that ban abortion. Despite advertising in Texas, we could not recruit any participants from that state, though we interviewed someone from Texas who felt it influenced their current practices. We note, however, that we did recruit a number of participants from Michigan—likely because we advertised on Twitter and one of the authors is in Michigan—where abortion is on the ballot in the Fall [11].

REFERENCES

[1] Alessandro Acquisti. 2009. Nudging Privacy: The Behavioral Economics of Personal Information. *IEEE Secur. Priv.* 7, 6 (November 2009), 82–85. DOI:https://doi.org/10.1109/MSP.2009.163

[2] Najd Alfawzan, Markus Christen, Giovanni Spitale, and Nikola Biller-Andorno. 2022. Privacy, Data Sharing, and Data Security Policies of

Women's mHealth Apps: Scoping Review and Content Analysis. *JMIR MHealth UHealth* 10, 5 (May 2022), e33735. DOI:https://doi.org/10.2196/33735

[3] 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), Association for Computing Machinery, New York, NY, USA, 1–5. DOI:https://doi.org/10.1145/3547522.3547674

[4] Nazanin Andalibi. 2020. Disclosure, Privacy, and Stigma on Social Media: Examining Non-Disclosure of Distressing Experiences. *ACM Trans. Comput.-Hum. Interact. TOCHI* 27, 3 (2020), 1–43.

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

[6] Nazanin Andalibi, Ashley Lacombe-Duncan, Lee Roosevelt, Kylie Wojciechowski, and Cameron Giniel. 2022. LGBTQ Persons' Use of Online Spaces to Navigate Conception, Pregnancy, and Pregnancy Loss: An Intersectional Approach. *ACM Trans. Comput.-Hum. Interact.* 29, 1 (January 2022), 2:1-2:46. DOI:https://doi.org/10.1145/3474362

[7] Nazanin Andalibi, Margaret E. Morris, and Andrea Forte. 2018. Testing Waters, Sending Clues: Indirect Disclosures of Socially Stigmatized Experiences on Social Media. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (November 2018), 19:1-19:23. DOI:https://doi.org/10.1145/3274288

[8] Sara Balderas-Díaz, María José Rodríguez-Fórtiz, José Luis Garrido, Mercedes Bellido-González, and Gabriel Guerrero-Contreras. 2021. Design of an Adaptable mHealth System Supporting a Psycho-educational Program for Pregnant Women with SGA Foetuses. In *Advances in Conceptual Modeling: ER 2021 Workshops CoMoNoS, EmpER, CMLS St. John's, NL, Canada, October 18–21, 2021, Proceedings*, Springer-Verlag, Berlin, Heidelberg, 125–135. DOI:https://doi.org/10.1007/978-3-030-88358-4_11

[9] Susan B. Barnes. 2006. A privacy paradox: Social networking in the United States. *First Monday* 11, 9 (September 2006). Retrieved December 5, 2017 from http://firstmonday.org/ojs/index.php/fm/article/view/1394

[10] Jerry Beilinson. 2020. Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds. *Consumer Reports*. Retrieved August 4, 2022 from https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats-a1100919965/

[11] Kim Bellware. Michigan abortion ballot measure will be put to voters in November. *Washington Post*. Retrieved October 5, 2022 from https://www.washingtonpost.com/nation/2022/09/08/michigan-supreme-court-abortion/

[12] Rasika Bhalerao, Nora McDonald, Hanna Barakat, Vaughn Hamilton, Damon McCoy, and Elissa M. Redmiles. 2022. Ethics and Efficacy of Unsolicited Anti-Trafficking SMS Outreach. (February 2022). Retrieved February 22, 2022 from https://arxiv.org/abs/2202.09527v1

[13] Emma Bowman. 2022. As states ban abortion, the Texas bounty law offers a way to survive legal challenges. *NPR*. Retrieved October 5, 2022 from https://www.npr.org/2022/07/11/1107741175/texas-abortion-bounty-law

[14] danah boyd. 2014. *It's Complicated: The Social Lives of Networked Teens* (1 edition ed.). Yale University Press.

[15] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qual. Res. Psychol.* 3, 2 (2006), 77–101. DOI:https://doi.org/10.1191/1478088706qp063oa

[16] Virginia Braun and Victoria Clarke. 2012. Thematic analysis. In *APA handbook of research methods in psychology, Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological*. American Psychological Association, Washington, DC, US, 57–71. DOI:https://doi.org/10.1037/13620-004

[17] Virginia Braun and Victoria Clarke. 2019. Reflecting on reflexive thematic analysis. *Qual. Res. Sport Exerc. Health* 11, 4 (August 2019), 589–597. DOI:https://doi.org/10.1080/2159676X.2019.1628806

[18] Sarah Brayne. 2020. Enter the Dragnet. *Log. Mag.* 12 (2020). Retrieved May 18, 2022 from https://logicmag.io/commons/enter-the-dragnet/

[19] Thomas Brewster. 15 Million Downloaded Pregnancy Trackers That May Give Data To Cops Without A Warrant—Should You Worry? *Forbes*. Retrieved August 4, 2022 from https://www.forbes.com/sites/thomasbrewster/2022/06/29/ziff-davis-pregnancy-trackers-may-give-data-to-cops-without-a-warrant/

[20] Khiara M. Bridges. 2017. *The Poverty of Privacy Rights* (1 edition ed.). Stanford Law Books, Stanford, California.

[21] Simone Browne. 2015. *Dark Matters: On the Surveillance of Blackness*. Duke University Press Books, Durham.

[22] Finn Brunton and Helen Nissenbaum. 2016. *Obfuscation: A User's Guide for Privacy and Protest* (Reprint edition ed.). The MIT Press, Cambrigde, Massachusetts London.

[23] US Census Bureau. *The Chance That Two People Chosen at Random Are of Different Race or Ethnicity Groups Has Increased Since 2010*. Retrieved October 5, 2022 from https://www.census.gov/library/stories/2021/08/2020-united-states-population-more-racially-ethnically-diverse-than-2010.html

[24] Albert Fox Cahn and Eleni Manis. 2022. *Pregnancy Panopticon: Abortion Surveillance After Roe*. Retrieved February 14, 2023 from https://www.stopspying.org/pregnancy-panopticon

[25] Beenish M. Chaudhry, Louis Faust, and Nitesh V. Chawla. 2019. From Design to Development to Evaluation of a Pregnancy App for Low-Income Women in a Community-Based Setting. In *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services* (MobileHCI '19), Association for Computing Machinery, New York, NY, USA, 1–11. DOI:https://doi.org/10.1145/3338286.3340118

[26] Patricia Hill Collins. 1990. *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment* (1st edition ed.). Routledge, New York, NY.

[27] Patricia Hill Collins. 2015. Intersectionality's Definitional Dilemmas. *Annu. Rev. Sociol.* 41, 1 (2015), 1–20.

[28] Patricia Hill Collins. 2019. *Intersectionality as Critical Social Theory*. Duke University Press Books, Durham.

[29] Patricia Hill Collins and Sirma Bilge. 2016. *Intersectionality* (1 edition ed.). Polity, Cambridge, UK ; Malden, MA.

[30] Nick Couldry and Ulises A. Mejias. 2019. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.

[31] Nick Couldry and Ulises A. Mejias. 2019. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Telev. New Media* 20, 4 (May 2019), 336–349. DOI:https://doi.org/10.1177/1527476418796632

[32] Joseph Cox. 2022. Data Broker Is Selling Location Data of People Who Visit Abortion Clinics. *Motherboard Tech by Vice*. Retrieved May 13, 2022 from https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood

[33] Kimberle Crenshaw. 1991. Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Rev.* 43, 6 (1991), 1241–1299.

[34] Michael A. DeVito, Ashley Marie Walker, and Jeremy Birnholtz. 2018. "Too Gay for Facebook": Presenting LGBTQ+ Identity Throughout the Personal Social Media Ecosystem. *Proc ACM Hum-Comput Interact* 2, CSCW (November 2018), 44:1-44:23. DOI:https://doi.org/10.1145/3274313

[35] Anna Diakun and Carrie DeCell. Perspective | Why is the U.S. still probing foreign visitors' social media accounts? *Washington Post*. Retrieved August 19, 2022 from https://www.washingtonpost.com/outlook/2022/04/26/social-media-surveillance-us-visas-state/

[36] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New Media Soc.* 21, 8 (August 2019), 1824–1839. DOI:https://doi.org/10.1177/1461444819833331

[37] Charles Duhigg. 2012. How Companies Learn Your Secrets - The New York Times. *New York Times Magazine*. Retrieved August 1, 2022 from https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp

[38] Virginia Eubanks. 2006. Technologies of Citizenship: Surveillance and Political Learning in the Welfare System. In *Surveillance and Security*, Torin Monahan (ed.). Routledge. DOI:https://doi.org/10.4324/9780203957257-12

[39] Virginia Eubanks. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press, New York, NY.

[40] Eliza Fawcett. 2022. Georgia's 6-Week Abortion Ban Begins Immediately After Court Ruling. *The New York Times*. Retrieved September 19, 2022 from https://www.nytimes.com/2022/07/20/us/georgia-abortion-ban.html

[41] Andrew Guthrie Ferguson. 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press, New York.

[42] Andrew Guthrie Ferguson. 2018. *Illuminating Black Data Policing*. Social Science Research Network, Rochester, NY. Retrieved August 1, 2019 from https://papers.ssrn.com/abstract=3142263

[43] Andrea Forte, Nazanin Andalibi, and Rachel Greenstadt. 2017. Privacy, Anonymity and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*.

[44] Michel Foucault. 1976. *The History of Sexuality, Vol. 1: An Introduction* (Reissue edition ed.). Vintage, New York.

[45] Michel Foucault. 1977. *Discipline & Punish: The Birth of the Prison*. Vintage Books, New York.

[46] Sarah Fox, Amanda Menking, Stephanie Steinhardt, Anna Lauren Hoffmann, and Shaowen Bardzell. 2017. Imagining Intersectional Futures: Feminist Approaches in CSCW. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '17 Companion), ACM, New York, NY, USA, 387–393. DOI:https://doi.org/10.1145/3022198.3022665

[47] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI'18), Association for Computing Machinery, New York, NY, USA, 1–13. DOI:https://doi.org/10.1145/3173574.3174241

[48] Gary Gates. 2017. Vermont Leads States in LGBT Identification. *Gallup.com*. Retrieved October 5, 2022 from https://news.gallup.com/poll/203513/vermont-leads-states-lgbt-identification.aspx

[49] Gennie Gebhart and Daly Barnett. 2022. Should You Really Delete Your Period Tracking App? *Electronic Frontier Foundation*. Retrieved August 19, 2022 from https://www.eff.org/deeplinks/2022/06/should-you-really-delete-your-period-tracking-app

[50] Angelica Goetzen, Samuel Dooley, and Elissa M. Redmiles. 2022. Ctrl-Shift: How Privacy Sentiment Changed from 2019 to 2021. DOI:https://doi.org/10.48550/arXiv.2110.09437

[51] Alice Goffman. 2014. *On the Run: Fugitive Life in an American City*. University of Chicago Press, Chicago ; London.

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

[53] Xinning Gui, Yu Chen, Yubo Kou, Katie Pine, and Yunan Chen. 2017. Investigating support seeking from peers for pregnancy in online health communities. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW (2017), 1–19.

[54] Jessica Smartt Gullion. 2015. *Writing Ethnography* (1st edition ed.). Sense Publishers.

[55] Eszter Hargittai and Alice Marwick. 2016. "What can I really do?" Explaining the privacy paradox with online apathy. *Int. J. Commun.* 10, (2016), 3737–3757.

[56] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical Computer Security for Victims of Intimate Partner Violence. 105–122. Retrieved October 6, 2022 from https://www.usenix.org/conference/usenixsecurity19/presentation/havron

[57] Kashmir Hill. 2022. Deleting Your Period Tracker Won't Protect You. *The New York Times*. Retrieved August 17, 2022 from https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html

[58] Kashmir Hill. You Can Hide Your Pregnancy Online, But You'll Feel Like A Criminal. *Forbes*. Retrieved August 1, 2022 from https://www.forbes.com/sites/kashmirhill/2014/04/29/you-can-hide-your-pregnancy-online-but-youll-feel-like-a-criminal/

[59] Lil Kalish. Meet abortion bans' new best friend: your phone. *Mother Jones*. Retrieved August 5, 2022 from https://www.motherjones.com/politics/2022/02/meet-abortion-bans-new-best-friend-your-phone/

[60] Reshmashree B. Kantharaju, Dominic De Franco, Alison Pease, and Catherine Pelachaud. 2018. Is Two Better than One? Effects of Multiple Agents on User Persuasion. In *Proceedings of the 18th International Conference on Intelligent Virtual Agents* (IVA '18), Association for Computing Machinery, New York, NY, USA, 255–262. DOI:https://doi.org/10.1145/3267851.3267890

[61] Eleanor Klibanoff. 2022. Texans who perform abortions now face up to life in prison, $100,000 fine. *The Texas Tribune*. Retrieved October 5, 2022 from https://www.texastribune.org/2022/08/25/texas-trigger-law-abortion/

[62] Neha Kumar and Naveena Karusala. 2019. Intersectional Computing. *Interactions* 26, 2 (February 2019), 50–54.

[63] Neha Kumar, Naveena Karusala, Azra Ismail, and Anupriya Tuli. 2020. Taking the Long, Holistic, and Intersectional View to Women's Wellbeing. *ACM Trans. Comput.-Hum. Interact.* 27, 4 (July 2020), 23:1-23:32. DOI:https://doi.org/10.1145/3397159

[64] Ron Lieber and Tara Siegel Bernard. 2022. Payment Data Could Become Evidence of Abortion, Now Illegal in Some States. *The New York Times*. Retrieved September 20, 2022 from https://www.nytimes.com/2022/06/29/business/payment-data-abortion-evidence.html

[65] Alice Marwick. 2022. Privacy Without Power: What Privacy Research Can Learn from Surveillance Studies. *Surveill. Soc.* 20, 4 (December 2022), 397–405. DOI:https://doi.org/10.24908/ss.v20i4.16009

[66] Alice Marwick, Claire Fontaine, and danah boyd. 2017. "Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, and Personal Responsibility Among Low-SES Youth. *Soc. Media Soc.* 3, 2 (April 2017). Retrieved February 14, 2018 from https://doi.org/10.1177/2056305117710455

[67] Leslie McCall. 2005. The Complexity of Intersectionality. *Signs* 30, 3 (2005), 1771–1800. DOI:https://doi.org/10.1086/426800

[68] 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*, Association for Computing Machinery, New York, NY, USA, 1–14. Retrieved August 26, 2021 from https://doi.org/10.1145/3313831.3376167

[69] Nora McDonald and Andrea Forte. 2021. Powerful Privacy Norms in Social Network Discourse. *PACM Hum.-Comput. Interact. CSCW* 5, 2 (2021).

[70] Nora McDonald and Andrea Forte. 2022. Privacy and Vulnerable Populations. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes and Jennifer Romano (eds.). Springer International Publishing, Cham, 337–363. DOI:https://doi.org/10.1007/978-3-030-82786-1_15

[71] Nora McDonald, Rachel Greenstadt, and Andrea Forte. accepted. Intersectional Thinking about PETs: A Study of Library Privacy.

[72] Corynne McSherry and Kathrine Trendacosta. 2022. What Companies Can Do Now to Protect Digital Rights In A Post-Roe World. *Electronic Frontier Foundation*. Retrieved August 19, 2022 from https://www.eff.org/deeplinks/2022/05/what-companies-can-do-now-protect-digital-rights-post-roe-world

[73] Maryam Mehrnezhad and Teresa Almeida. 2021. Caring for Intimate Data in Fertility Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (CHI '21), Association for Computing Machinery, New York, NY, USA, 1–11. DOI:https://doi.org/10.1145/3411764.3445132

[74] Margi Murphy. 2022. Anti-Abortion Centers Find Pregnant Teens Online, Then Save Their Data. *Bloomberg.com*. Retrieved August 1, 2022 from https://www.bloomberg.com/news/articles/2022-06-27/anti-abortion-centers-find-pregnant-teens-online-then-save-their-data

[75] Naomi Nix and Elizabeth Dwoskin. 2022. Search warrants for abortion data leave tech companies few options. *Washington Post*. Retrieved September 20, 2022 from https://www.washingtonpost.com/technology/2022/08/12/nebraska-abortion-case-facebook/

[76] Katy E. Pearce, Amy Gonzales, and Brooke Foucault Welles. 2020. Introduction: Marginality and Social Media. *Soc. Media Soc.* 6, 3 (July 2020), 2056305120930413. DOI:https://doi.org/10.1177/2056305120930413

[77] Tamara Peyton, Erika Poole, Madhu Reddy, Jennifer Kraschnewski, and Cynthia Chuang. 2014. Information, sharing and support in pregnancy: addressing needs for mHealth design. In *Proceedings of the companion publication of the 17th ACM conference on Computer supported cooperative work & social computing* (CSCW Companion '14), Association for Computing Machinery, New York, NY, USA, 213–216. DOI:https://doi.org/10.1145/2556420.2556489

[78] Tamara Peyton, Erika Poole, Madhu Reddy, Jennifer Kraschnewski, and Cynthia Chuang. 2014. "Every pregnancy is different": designing mHealth for the pregnancy ecology. In *Proceedings of the 2014 conference on Designing interactive systems* (DIS '14), Association for Computing Machinery, New York, NY, USA, 577–586. DOI:https://doi.org/10.1145/2598510.2598572

[79] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. 2022. Replication: Stories as Informal Lessons about Security. 1–18. Retrieved October 10, 2022 from https://www.usenix.org/conference/soups2022/presentation/pfeffer

[80] The Associated Press. 2022. Oklahoma governor signs the nation's strictest abortion ban. *NPR*. Retrieved October 5, 2022 from https://www.npr.org/2022/05/26/1101428347/oklahoma-governor-signs-the-nations-strictest-abortion-ban

[81] Cassidy Pyle, Lee Roosevelt, Ashley Lacombe-Duncan, and Nazanin Andalibi. 2021. LGBTQ Persons' Pregnancy Loss Disclosures to Known Ties on Social Media: Disclosure Decisions and Ideal Disclosure Environments. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (CHI '21), Association for Computing Machinery, New York, NY, USA, 1–17. DOI:https://doi.org/10.1145/3411764.3445331

[82] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (SOUPS '12), Association for Computing Machinery, New York, NY, USA, 1–17. DOI:https://doi.org/10.1145/2335356.2335364

[83] Yolanda A. Rankin and Jakita O. Thomas. 2019. Straighten Up and Fly Right: Rethinking Intersectionality in HCI Research. *Interactions* 26, 6 (October 2019), 64–68.

[84] VIctor M. Rios. 2011. *Punished: Policing the Lives of Black and Latino Boys (New Perspectives in Crime, Deviance, and Law) - Kindle edition by*

Victor M. Rios. Politics & Social Sciences Kindle eBooks @ Amazon.com. NYU Press, New York. Retrieved February 14, 2018 from https://www.amazon.com/Punished-Policing-Latino-Perspectives-Deviance-ebook/dp/B005C9GOCM/ref=sr_1_1?ie=UTF8&qid=1518664844&sr=8-1&keywords=punished+policing

[85] Alfred Schutz. 1967. *The Phenomenology of the Social World*. Northwestern University Press.

[86] Sophia Cope and Adam Schwartz. 2017. DHS Should Stop the Social Media Surveillance of Immigrants. *Electronic Frontier Foundation*. Retrieved February 27, 2019 from https://www.eff.org/deeplinks/2017/10/dhs-should-stop-social-media-surveillance-immigrants

[87] Laura Shipp and Jorge Blasco. 2020. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proc. Priv. Enhancing Technol.* 2020, 4 (October 2020), 491–510. DOI:https://doi.org/10.2478/popets-2020-0083

[88] Natasha Singer and Brian X. Chen. 2022. In a Post-Roe World, the Future of Digital Privacy Looks Even Grimmer. *The New York Times*. Retrieved July 30, 2022 from https://www.nytimes.com/2022/07/13/technology/personaltech/abortion-privacy-roe-surveillance.html

[89] Wally Smith, Greg Wadley, Oliver Daly, Marianne Webb, Jo Hughson, John Hajek, Anna Parker, Robyn Woodward-Kron, and David Story. 2017. Designing an app for pregnancy care for a culturally and linguistically diverse community. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction* (OZCHI '17), Association for Computing Machinery, New York, NY, USA, 337–346. DOI:https://doi.org/10.1145/3152771.3152807

[90] Tierney Sneed. Some states move quickly to ban abortion after Supreme Court ruling. *CNN*. Retrieved September 19, 2022 from https://www.cnn.com/2022/06/24/politics/abortion-ban-states-move-quickly/index.html

[91] Daniel Solove. 2020. The Myth of the Privacy Paradox. *GW Law Fac. Publ. Works* (January 2020). Retrieved from https://scholarship.law.gwu.edu/faculty_publications/1482

[92] Andrew Ross Sorkin, Vivian Giang, Stephen Gandel, Lauren Hirsch, Ephrat Livni, and Jenny Gross. 2022. Reconsidering Privacy Risks After Roe. *The New York Times*. Retrieved July 30, 2022 from https://www.nytimes.com/2022/06/30/business/dealbook/abortion-privacy-risks-data.html

[93] Jakita O. Thomas, Nicole Joseph, Arian Williams, Chan'tel Crum, and Jamika Burge. 2018. Speaking Truth to Power: Exploring the Intersectional Experiences of Black Women in Computing. In *2018 Research on Equity and Sustained Participation in Engineering, Computing, and Technology (RESPECT)*, 1–8. DOI:https://doi.org/10.1109/RESPECT.2018.8491718

[94] Rina Torchinsky. 2022. How period tracking apps and data privacy fit into a post-Roe v. Wade climate. *NPR*. Retrieved September 20, 2022 from https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps

[95] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2020. The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums.

[96] Joseph Turow, Michael Hennessy, and Nora Draper. 2015. The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation. DOI:https://doi.org/10.2139/ssrn.2820060

[97] Janet Vertesi. 2014. My Experiment Opting Out of Big Data Made Me Look Like a Criminal. *Time*. Retrieved August 1, 2022 from https://time.com/83200/privacy-internet-big-data-opt-out/

[98] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. 'I Knew It Was Too Good to Be True": The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proc ACM Hum-Comput Interact* 2, CSCW (November 2018), 176:1-176:25. DOI:https://doi.org/10.1145/3274445

[99] Gerrit De Vynck, Caroline O'Donovan, Tiku, and Elizabeth Dwoskin. 2022. Abortion is illegal for millions. Will Big Tech help prosecute it? *Washington Post*. Retrieved September 20, 2022 from https://www.washingtonpost.com/technology/2022/06/29/google-facebook-abortion-data/

[100] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A field trial of privacy nudges for facebook. 2367–2376.

[101] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. 2022. SoK: A Framework for Unifying At-Risk User Research. In *2022 IEEE Symposium on Security and Privacy (SP)*, 2344–2360. DOI:https://doi.org/10.1109/SP46214.2022.9833643

[102] Nicole Wetsman and Victoria Song. 2022. How to delete your period tracking app data. *The Verge*. Retrieved August 19, 2022 from https://www.theverge.com/2022/6/30/23190142/delete-period-tracking-app-roe-v-wade-how-to

[103] Pamela J. Wisniewski, Bart P. Knijnenburg, and Heather Richter Lipford. 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. *Int. J. Hum.-Comput. Stud.* 98, (February 2017), 95–108. DOI:https://doi.org/10.1016/j.ijhcs.2016.09.006

[104] Pamela J. Wisniewski, Neha Kumar, Christine Bassem, Sarah Clinch, Susan M. Dray, Geraldine Fitzpatrick, Cliff Lampe, Michael Muller, and Anicia N. Peters. 2018. Intersectionality As a Lens to Promote Equity and Inclusivity Within SIGCHI. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI EA '18), ACM, New York, NY, USA. Retrieved July 25, 2018 from http://doi.acm.org/10.1145/3170427.3186324

[105] Shoshana Wodinsky and Kyle Barr. 2022. These Companies Know You're Pregnant—And They're Not Keeping It Secret. *Gizmodo*. Retrieved August 4, 2022 from https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426

[106] Kate Zernike. 2022. Ohio Judge Temporarily Suspends Abortion Ban. *The New York Times*. Retrieved September 19, 2022 from https://www.nytimes.com/2022/09/14/us/ohio-abortion-ban-suspended.html

[107] Shoshana Zuboff. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *J. Inf. Technol.* 30, 1 (March 2015), 75–89.

[108] Shoshana Zuboff. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (1 edition ed.). PublicAffairs, New York.

[109] 2016. Abortion in Texas. *ACLU of Texas*. Retrieved October 5, 2022 from https://www.aclutx.org/en/know-your-rights/abortion-texas

[110] 2021. Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data. *Federal Trade Commission*. Retrieved August 4, 2022 from https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about

[111] 2022. Readout of White House Listening Session on Tech Platform Accountability. *The White House Briefing Room*. Retrieved September 13, 2022 from https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/08/readout-of-white-house-listening-session-on-tech-platform-accountability/

[112] Revolting Prostitutes: The Fight for Sex Workers' Rights - Kindle edition by Smith, Molly, Mac, Juno. Politics & Social Sciences Kindle eBooks @ Amazon.com. Retrieved October 5, 2022 from https://www.amazon.com/Revolting-Prostitutes-Fight-Workers-Rights-ebook/dp/B074DGPLM1/ref=sr_1_1?crid=H0KX2ZO7V3PP&keywords=sex+workers+molly&qid=1664995094&qu=eyJxc2MiOiIwLjcxIiwicXNhIjoiMC4wMCIsInFzcCI6IjAuMDAifQ%3D%3D&s=books&sprefix=sex+workers+moll%2Cstripbooks%2C55&sr=1-1

This paper has no relation whatsoever to prior papers by these authors.