Reproductive Security & Privacy Advice on TikTok after the Overturn of Roe

Harshini Sri Ramulu
Paderborn University

Rachel Gonzalez Rodriguez
Paderborn University

Yasemin Acar
Paderborn University

Lucy Simko
Barnard College

Abstract

In 2022, the Supreme Court of the United States overturned Roe v. Wade, a seminal case linking the right to privacy to the right to reproductive self determination at the federal level. Reproductive self determination in the US is now regulated at the state level, with vast differences across states. With the current landscape of online tracking, people who may become pregnant are at risk of prosecution based on data from their digital footprint, including online searches, period trackers, and fitness trackers. After the overturn of Roe v. Wade, social media creators reacted on TikTok, including by giving security and privacy advice regarding reproductive health under the new legal situation.

To empower vulnerable users to protect their security and privacy, we need to understand the landscape of security and privacy advice immediately after significant shifts in legislation. We qualitatively analyze 92 TikTok videos giving advice on reproductive security and privacy after the overturn of Roe v. Wade. We find that content creators connected general-purpose security advice (like using encrypted messengers) to reproductive privacy, and that domain-specific advice (like abandoning period tracking apps) emerged. Though each piece of advice was often *sound*, it collectively lacked nuance, actionability, completeness, and practicality due to the complexities of the legal, technical, and interpersonal threat landscape. We provide recommendations for advice-givers, social media platforms, and the security community, towards stronger, more actionable, and more complete communication of domain-specific security and privacy advice during crisis.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

1 Introduction

There are myriad apps, websites, and online search tools that individuals may turn to while managing reproductive health. For example, one might track their menstrual cycle with a period tracking app, use a search engine to locate an abortion clinic, navigate to a prenatal appointment using a navigation app, or seek support on social media after a miscarriage. These activities generate vast amounts of digital data documenting pregnancy and loss, some of which can be accessed by law enforcement [73], and have recently been leveraged to prosecute pregnancy terminations [57, 66].

While these threats to privacy have existed for years, many in the US experienced a significant shift in risk after the Supreme Court removed the federal protection of abortion rights established by Roe v. Wade, allowing states to immediately regulate access to reproductive care, including abortion [92]. At the time of writing in February 2026, 17 states have enacted near-total abortion bans or bans at 6 weeks, and 11 states impose restrictions in the second trimester [2]; these restrictions both endanger pregnant people who cannot access care, and incentivize them to access care illegally [67].

The abrupt changes in the legal status of reproductive healthcare created a landscape in which the vast digital footprint created by normative technology use put pregnant people in some states at risk for prosecution and harassment. In response, viral security and privacy advice flooded news and social media after the overturn, with urgent calls to, for example, delete period tracking apps [42] and travel phonelessly or with a burner phone to an abortion clinic [34]. However, due to the magnitude of data available to US law enforcement through any number of US-based corporations and data brokers, *no single strategy can provide privacy for someone seeking an abortion in a restricted state.*

Because of the impossibility of *complete* reproductive privacy, different strategies are important for different people [72, 73], and it is therefore critical to understand the nature and quality of the privacy advice circulating right after the overturn of Roe as it reflects the collective sense-making that

aimed to shape reproductive privacy and security. Given TikTok's popularity with young adults and teens [21], who are more likely to experience unwanted pregnancy [137], we studied advice *on TikTok*, asking the following research questions:
RQ1: *After the overturn of Roe v. Wade, what security and privacy advice emerged on TikTok for people seeking reproductive care in the US?*
RQ2: *To what extent does this security and privacy advice (a) draw from existing privacy and security strategies, and (b) address threats to reproductive privacy in the US?*

Through an iterative search at the intersection of *security and privacy advice* and *reproductive health*, we qualitatively analyzed 92 TikTok videos. Advice to delete one's period tracking app was common, yet we find a wealth of *other* advice, e.g., about searching online without leaving a digital footprint, secure messaging, and avoiding location tracking. As prior work has documented in other times of geopolitical change, such as the US Black Lives Matter protests [19], the Russian invasion of Ukraine [107], and the Sudanese revolution [27], some advice is *"general-purpose" security advice* that content creators tailored here for reproductive health (e.g., using incognito mode to search for abortion care); other advice stemmed from *strategies to manage reproductive health*, tailored for privacy (e.g., recording one's period on paper to avoid data tracking). However, as a collection—and even moreso as piecemeal advice—it does not fully address the complex and varied threat landscape, nor does most of it adhere to best practices for presentation of security and privacy advice [65, 101]. Individually, it is aimed at those in the most risky situations, but gives little guidance on how to threat model, which is crucial for effective safety measures given the individual, geographic, and relational nature of risk to reproductive privacy [72, 73]. Our contributions:
(a) We catalog security and privacy advice that emerged on TikTok in response to the restricted access to reproductive healthcare in the US in 2022 (Table 1).
(b) We analyze how content creators both tailored general-purpose security and privacy advice to reproductive health, and presented some reproductive health management strategies as privacy-centric (Section 4).
(c) We make recommendations for advice-givers, social media platforms, and the security community for advice that leverages the engaging qualities of short viral videos, but aligns more closely with both present threats to privacy, and best practices for security advice (Section 5).

2 Background and Related Work

2.1 Background

Roe v. Wade (1973), a foundational privacy law in the US, connected bodily autonomy with the fourteenth[1] amendment [18] of the US Constitution, recognizing "*'the right of the individual...to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child...' includes the right of a woman to decide whether or not to terminate her pregnancy....the right asserted by Jane Roe is embraced within the personal liberty protected by the Due Process Clause of the Fourteenth Amendment*" [18]. In 2022, however, the Supreme Court determined that "*Roe ... must be overruled. The Constitution makes no reference to abortion, and no such right is implicitly protected by any constitutional provision*" [120]. Here, we briefly summarize the impacts of this overturn.

Rapidly changing availability of reproductive healthcare. The plan to overturn Roe v. Wade was leaked in May 2022. Despite public outcry, the Supreme Court overturned it a month later, in June 2022. The legal landscape changed overnight, as 13 states had pre-enacted *trigger laws* [55, 84], so named because they go into effect after a triggering event, immediately[2] restricting access to abortion care. Legislation has continued to change. For example, in Montana, an unsuccessful bill was proposed to criminalize "abortion trafficking:" purposely or knowingly transporting "*an unborn child that is currently located in this state either to a location within this state or to a location outside of this state with the intent to obtain an abortion that is illegal in this state*" [20].

Prosecution of people who sought abortion. The new legal landscape enables prosecution of those who seek abortions. As of October 2024, there had been over 200 cases of prosecution because of pregnancy or pregnancy loss [130]. Use of digital evidence to prosecute abortion-seekers is currently rare, despite both the public movement towards digital reproductive privacy [24, 34, 42, 72, 74, 86, 108] and the copious documentation of pregnancy and pregnancy loss during normative technology use. While there is no comprehensive database of how digital evidence has been used in abortion prosecution cases, (unencrypted) Facebook messages [57] and screenshots of text messages [16] have both been used as evidence against people who allegedly sought illegal abortions. Despite the rarity, our research is critical because of how public conversation may shape mental models and security and privacy strategies during a changing political situation.

The cost of abortion bans goes far beyond prosecution of abortion-seekers. Restricted access to abortions also affects treatment for miscarriages and spontaneous abortions, a natural process that occurs in 10-15% of early pregnancies [115]. Since 80% of spontaneous abortions happen in the

[1] "*No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.*" [64]

[2] In Kentucky, Louisiana and South Dakota, once the overturn occurred, the bans immediately went into effect. In Idaho, Tennessee, and Texas, there was a 30 day delay. In Arkansas, Mississippi, Missouri, North Dakota, Oklahoma, Utah, and Wyoming, the trigger laws required government approval after the overturn; in these states, near-total bans are enacted, or providers have ceased service [55, 84].

first trimester [115], some restrictions criminalize medically necessary interventions [26].

Abortion providers, too, are at risk. In January 2025, prosecution of an abortion provider led to the first "*criminal... charges for providing abortion pills across state lines*" [134] for a doctor in New York who had mailed medical abortion pills to an out of state patient who then tried to provide them to their underage daughter in a state with a complete abortion ban [134]. Additionally, the number of abortions in the United States has *increased* since the overturn of Roe v. Wade. The Guttmacher Institute states that "*over 170,000 patients traveled out of state in 2023 to seek abortion care. Individuals traveling across state borders must overcome significant economic and logistical barriers. We also know that many others were unable to obtain care in the formal health care system, and some were forced to continue their pregnancies*" [67].

2.2 Related work

Prior work has extensively studied the security and privacy concerns of various at-risk and marginalized groups [126], including immigrants and refugees [44, 111, 124], incarcerated people [88, 89], activists [19, 27], sex workers [45, 112], human trafficking survivors [25], survivors of abuse [40, 87, 132], children [60, 61] and older adults [41, 76, 77, 83, 95–97] (all of whom may require reproductive care in the US). Prior work also highlights that security and privacy are not always a priority [82, 104, 111, 124], and some groups, like sex workers, mention that the solutions currently available are insufficient [14, 71, 112]. Recent scholarship shows that people who may become pregnant in the post-Roe era are at risk of having their privacy and safety compromised [72], and intersectional identities cause some of the groups above to be particularly vulnerable when access to abortion and other reproductive care is restricted [29, 56, 118]. Our work complements previous studies and aims to understand the landscape of perceived security and privacy threats for people seeking reproductive healthcare in the post-Roe era.

Reproductive technology. Prior HCI research on concerns around reproductive health majorly focused on reproductive health tracking apps (called FemTech, FemHealth, or mHealth apps) [7, 24, 48, 68, 74]. FemHealth apps help those who menstruate track their health. Extensive research in HCI discusses benefits of FemHealth apps [54, 63, 123]; however, several studies in security and privacy reveal issues with these apps, like data breaches [75, 102], security vulnerabilities [32], obscure privacy policies [39], and excessive data sharing with third parties [72, 79, 108, 113].

Post-Roe, studies have investigated users' perceptions of and concerns with FemHealth apps, finding that users are concerned about privacy practices, especially data sharing with law enforcement and third parties [24, 74]. Prior work has shown that users lack awareness of how their FemHealth data is handled due to non-transparent data handling processes [24]. Additionally, users from cultures where menstruation is taboo have indicated privacy issues with these apps [51, 125]. After the 2022 Roe v. Wade overturn, US users are increasingly concerned about privacy issues surrounding FemHealth apps [86, 108]; some have deleted them [24, 72]. Although menstruation apps are an important topic, McDonald and Andalibi argue that focusing on FemHealth apps *alone* provides a narrow outlook of threats posed by the entire technical and legislative landscape [72]. There has been limited prior work on reproductive privacy and security outside menstruation apps, including work about online abortion clinics. These services offer benefits to people for whom in-person care is not possible (e.g., by sending abortion pills via mail) [4], but can still be inaccessible to marginalized groups and minors [58]. These services have sold user data to third parties [24]. Our study adds to existing work by identifying how security and privacy advice relating to reproductive health care proliferates online.

Security and privacy advice. Previous work has extensively explored various aspects of security advice, including where users seek advice and what influences them to follow it: People rely on various sources for advice but prefer websites [98, 100], and they trust advice that comes from security professionals [99] not loaded with marketing material [46, 99]. Prior work found differences in advice from experts and non-experts [23, 53]. Both experts and non-experts struggle with prioritizing advice [85, 101], consistent with findings that security advice is hard to follow, inconsistent, and difficult to prioritize [100, 101]. Schmüser et al. suggest tailoring advice to specific groups and situations rather than bombarding people with large amounts of advice at once, which becomes a problem in crises [107]. Social media can be an effective medium to disseminate security and privacy advice [17]; previous work has explored discourse on specific topics like mental health [37], menstrual health [114], war [107], anti-security advice [133], protests [19], and sexual abuse [131].

Following the overturn of Roe v. Wade, social media has been increasingly used for reproductive health information [127], though Song et al. (in a study of Reddit) note that information is sometimes based on speculation [114]. Song et al. also find that reproductive health companies use social media to reassure users about privacy practices, as well as to promote their products [113]. Social media has been a vital tool in raising awareness regarding privacy issues, legal implications, and general discourse on reproductive rights [28]. Building on prior work related to security and privacy advice and post-Roe discourse on social media, we analyze the content and quality of security and privacy advice on TikTok after the fall of Roe.

3 Methods

Social media analysis is a powerful tool to understand communities by collecting data *in situ*, allowing researchers to see

advice as it is presented to others. Prior work, particularly in *crisis informatics* [90], has leveraged social media analysis to explore online community reactions to and mutual aid during disasters [50, 129]. Similarly, security and privacy research has leveraged social media analysis to investigate advice following disruptive events [62, 107]. Here, we explore how TikTok users provide privacy advice to people seeking reproductive healthcare after the overturn of Roe v. Wade. Due to the sensitive nature of our research, we carefully considered ethics at all stages, detailed in Section 3.3.

Research on Tiktok. TikTok is a social media platform especially popular with people aged 18-34 [116]. On TikTok, content creators upload short videos and can take advantage of in-app editing to add video effects, audio tracks, or images or other videos (known as *stitching*). TikTok has received increasing attention from the usable security and privacy research community due to prolific (anti-)security advice and information relayed on the platform [106, 110, 117, 133]. Prior work shows that TikTok is influential on users' behaviors [81, 119]—although there is a risk of misinformation [78].

Dataset overview. We iteratively and systematically collected videos on TikTok (as in prior work [110, 133]) that gave advice about reproductive health and security and privacy, with a dataset of 92 videos. Most videos were posted between May 2022—when the overturn of Roe was leaked [116]—and February 2023; 9 are slightly older, with the oldest from January 2021, included because they would have been seen by casual TikTok viewers after the overturn as well.

3.1 Data scope and data collection

To focus our search, our *inclusion criteria* required videos to: (a) be about reproductive health, (b) be about privacy and/or security, and (c) give advice. Importantly, the *combination* of these criteria removed discussion focused on politics or morals, as our goal was to evaluate practical (or impractical) security advice.

To simulate the experience of someone in the US receiving reproductive privacy advice from TikTok, we collected the data while in the US, using fresh TikTok accounts on phones separate from our personal devices (to avoid targeting based on our advertising profiles). We collected data in February 2023, about eight months after Roe v. Wade was overturned.

Using our inclusion criteria, we iteratively conducted a hashtag-based search for relevant videos on TikTok. To begin our data collection, three researchers brainstormed an initial set of 6 hashtags. We included terms based on our own experiences on social media (e.g., #roevwade) as well as what we expected might be relevant terms (e.g., #abortion). Videos associated with these hashtags had over 15 billion views at the time of our data collection. Given this initial set of 6 hashtags, we entered an iterative process: two researchers iteratively searched for each hashtag, saved the top N videos (first round: N=30; subsequent rounds: N=20) from each hashtag, applied inclusion criteria, and extracted new hashtags from each video. We then iterated, using the new hashtags.

In total, our search of 61 iteratively-collected hashtags resulted in 1280 video search results (some duplicates), which two researchers watched, manually de-duplicated, and coded for relevancy using our previously determined inclusion criteria. Round 1 produced 18 relevant videos; round 2, 22; round 3, 36; and round 4, 6 videos, for a total of *82 videos collected from hashtag searches*. For each, we saved the relevant hashtags, keywords, view count, and downloaded the video if available. Finally, we conducted one additional search to identify videos that fit our inclusion criteria but were not labeled with hashtags: from the captions of the 82 videos, we manually curated search terms about reproductive health and privacy. These search terms resulted in 111 videos. Two researchers applied the inclusion criteria to these videos and found 10 new relevant videos, resulting in **92 total videos in our dataset**.

3.2 Data Analysis

To understand and characterize the security and privacy advice shared on TikTok after the overturn of Roe v. Wade, we conducted qualitative analysis of the 92 TikTok videos in our dataset. We used a deductive and inductive coding approach to develop our codebook. We created an initial deductive codebook based on security and privacy advice in the context of reproductive health advice commonly shared online (through Google search) and in prior work [7, 108]. As we started coding Tiktok videos, we inductively added new codes to represent advice not present in our initial codebook. Our codebook creation was informed by our experience as security and privacy researchers, with backgrounds in empirical, specifically qualitative research, and also one researcher's criminal justice background, as well as an awareness and familiarity with the US and social media (specifically TikTok) cultural landscape. Two researchers independently coded all the videos. They met regularly to resolve disagreements and iterated the codebook by adding new codes, merging codes, and deleting unused codes. Our codebook is appended (B). Additionally, we also took notes on all videos about tone, format, whether it was promotional content,[3] and recorded whether the video had issues with audio or text.

3.3 Ethics Statement

After careful considerations and discussions with the entire research team [59], we identified as the stakeholders in this research (a) the content creators who provided the videos we analyzed, (b) the research team, and (c) the broader community or public who may read or be impacted by our research. For (a), we carefully adhered to the principles of the Menlo

[3]We marked posts as promotional only when they were posted from the company's official account, which may have resulted in undercounting.

report [13] and best practices for handling public social media data [22, 38, 138]. We paraphrased creators' quotes to avoid any direct re-identification based on recent studies on social media [106, 110, 117, 133]; we explain our process for altering quotes in Appendix A. Further, we stored our data securely in a self-hosted cloud service. For (b), due to the nature of the research, and the long exposure to social media, we followed best practices for the safety of the research team [70], including limiting the frequency of data analysis sessions, regular debriefing within the research team, emotional wellness check-ins, and ensuring that researchers could stop analyzing data if they were emotionally burnt out. We do not foresee negative impacts through our research to (c), which helped us to decide to conduct this research.

Following the lead of prior work [106, 117, 133], we do not provide the full list of hashtags publicly, to reduce impact on the content creators in our dataset, who did not consent to being included in our research. In order to preserve the richness in our data, we generally do not redact well known company/app names throughout this paper, as future work could build off our work and evaluate their claims. We present content creators' claims as their own and do *not* endorse any specific technologies mentioned. However, we do redact the names of companies/apps containing promotional material or any other identifiable information in the quotes, because these could lead to re-identification since they are posted by the company and not by an unaffiliated individual. Because our data is public, our work did not fall under our institution's IRB.

3.4 Limitations

Necessarily, and appropriately given the US-based nature of the topic, our dataset is US-centric. Threats to reproductive privacy are shaped by legal, technical, societal landscapes, which differ around the world. People in other countries have differing levels of access to reproductive care, and those with restricted access may have similar communities of support and advice. We thoroughly encourage future researchers to work with and learn from those communities. Our view of the security and privacy advice shared around reproductive health in the US is necessarily limited by the platform we chose (TikTok), the search terms we used, and our focus on the top N videos for each search term. The public nature of TikTok, as well as TikTok's popularity with a certain demographic, means that other social media platforms may have different advice. It is also possible that people may post different advice privately than publicly. And although our search for videos was systematic, and we observed thematic convergence and therefore stopped searching, it is possible that starting with different seed terms could have led to a different dataset. Additionally, our focus was on videos with the highest engagement, so we may have missed insightful videos that lacked engagement or did not use the hashtags and keywords with which we searched. Further, we only collected videos in English. Videos not in the language of the majority may have different content. Our data is not longitudinal, so we have no insight into how advice may change over time, and we do not include analysis of users' reactions and perceptions.

Finally, we did not include coded language used on TikTok (similar to tactics for circumventing China's censorship [47]), which may have excluded videos. When we attempted this, results, if any, were drowned out by people discussing the original meaning of the coded words in earnest. For example, searching for variations of "going camping" yielded TikToks about camping, kayaking, etc.

4 Results

We find a wide variety of security and privacy advice on TikTok, reflecting the public collectively making sense of and responding to the immediate need for reproductive privacy after the fall of Roe. As a collection, the videos give security and privacy advice relevant to reproductive health, and educate viewers about legal, technical, and interpersonal threats in a post-Roe digital and physical surveillance landscape. Many content creators name law enforcement (or "the government") as the primary party that might access reproductive health data. Some also specify technical actors (like data brokers and tech companies) and interpersonal actors (like friends and family) as conduits for reproductive health data to law enforcement. Content creators gave goal-based advice: how to do (or how *not* to do) a specific reproductive health task *safely*, *securely*, and *privately*. Advice ranged from targeted and specific (e.g., use a specific menstruation app to protect data from government access) to general privacy advice without reasoning (e.g., always use a certain browser for privacy). Some present privacy tools; others advocate for technology non-use. Content creators applied general security and privacy advice to reproductive privacy—as in other crises or political movements [19, 27, 107]—and also newly positioned certain reproductive care strategies as private and secure. Although most advice accurately addresses high-level legal and technical threats posed by the role of technology in managing reproductive health, it does not comprehensively address threats to reproductive privacy in the post-Roe US.

Through the following subsections, we present content creators' privacy and security advice to users, centered around the problem that each piece of advice tries to solve (drawn qualitatively from our dataset): tracking periods (Section 4.1), obtaining health information (Section 4.2), and physically accessing abortion (Section 4.3). We present the advice without endorsement, and content creators' views *as their own*, using their language to identify threats from the perspective of someone seeking reproductive privacy. We note blatant (and rare) misinformation where it occurs. Throughout each advice-based section, we note where the advice echos security and privacy advice from other contexts. Additionally, while

a systematic evaluation of each piece of advice would be impossible due to the personal nature of risk, we assess how the advice aligns with or diverges from reproductive privacy threats that people in the US currently face.

Dataset description. Our dataset consisted of 92 TikToks from 82 unique creators, with the shortest video being six seconds and the longest being two minutes and 58 seconds. At the time of data collection, the videos collectively had 91 million views. Eight videos were marked as promotional content from four FemHealth companies, two of which were period trackers, one promoted online abortion pills, and one sold menstrual products; we coded videos as promotional if the video promoted a product and the account name matched the company's name. Four videos were posted by news agencies, one video by a lawyer, and two videos by companies who generally cautioned digital safety post Roe. Four videos were posted by health care professionals, and two each by: NGOs for reproductive health and academics. The creators of the remaining 59 videos did not make their professions public.

4.1 Advice about how (not) to track one's menstrual cycle

Menstruation tracking advice featured prominently in our dataset, with some advice recommending certain tracking strategies as safe, and some advocating for non-use of other tracking strategies for privacy. The emphasis on safe period tracking is unsurprising, as prior work also noted issues with companies like selling data to third parties or storing data on unencrypted servers [68]. As summarized in Table 1, period tracking advice was robust both in *strategies* and in explanations of *why* advice would increase privacy. Some content creators advised against *all* menstruation apps, others recommended deleting or using a specific app, and some instructed viewers to track their cycles outside an app. As a collection, the advice largely advocates for the *non-use* of technology, with generally nuanced explanations of what each measure protects from. However, as we discuss, private and secure period tracking does not cover *all* reproductive privacy needs, and videos did not acknowledge that safe period tracking is only one piece of a complex puzzle.

TikTok advice: Delete period tracking apps. The most common advice in our dataset was to stop using period tracking apps, with 18 videos advocating for non-use. 12 videos advised deleting *all* period tracking apps, and six named specific apps. Videos reasoned about government and corporate access to data, data mining, data breaches, and trust of the company.

Several videos advised viewers to delete apps due to the potential for government data access, e.g., "*in this economy it's probably not good to put all your data in a period tracking app because of the government*" (V6). A few videos instructed viewers to stop using *Stardust*, claiming it "*will hand over your data even if there isn't a warrant*" (V66). V85 stated that the same app, "*the Stardust period tracker app, which—after Roe v. Wade was overturned—lauded itself as a period tracker app that offered end-to-end encryption and definitely would not give data to the government. But later it was revealed that they would actually send your data to the government. After this came out, they just removed the claims of encryption from their privacy policy . . . Soooo, delete the app*" (V85). As we explore below, these claims are at odds with videos promoting specific apps, some of which are advertisements.

Others discussed data sharing with third parties as reason to delete period tracking apps. In V39, a creator reacts to a video from a period tracking app's social media account claiming coverage under GDPR [52]. V39 stated the app "*failed to mention something really important: your data is stored on Amazon web services in Ireland. Ireland's pretty well known for not following to those strict laws*" (V39). A few videos invoked general threats of data breaches: "*Should you delete your period tracking apps? Yeah probably, assuming you don't want people getting that information*" (V67).

Prior work has observed disuse of period tracking apps in response to privacy concerns after the overturn of Roe v. Wade [24], as well as non-use of technology in other contexts for ideological or philosophical reasons [8, 15, 105], including non-adoption of Internet of Things devices [43] and contact tracing apps [11] due to privacy concerns.

TikTok advice: Use a certain app for period tracking. Eight videos recommended certain menstruation apps as sufficiently private, presented by content creators seemingly unaffiliated with the app (we present self-promotional videos next). Most videos invoked the *lack* of data sharing (prevented by policy or design) as a reason to recommend apps (using similar reasoning to those calling for non-use of period tracking apps). Some also gave reasons other than privacy, such as the health benefits of menstruation tracking (e.g., fertility).

Three videos recommended apps for their data storage design and policies. V53 recommended *Clue* since it "*is in Europe*" (V53); V67 suggested *drip* because "*it only stores data on your actual phone, which gives you some protection from cloud-based access*" (V67); and V61 recommended Apple's *Health* app because "*courts might be able to subpoena data with the overturn of Roe v. Wade . . . the only way to prevent it is for apps to end-to-end encrypt your data. Apple's period tracking app is the only one that does this*" (V61).

These videos show a strong understanding of privacy best practices adhering to a model of a remote adversary that follows domestic and international law: recommending protection through the EU's GDPR, local data storage, and end-to-end encryption. Interestingly, the same app maligned for storing data in Ireland was one recommended for being in the EU.

TikTok advice: Use a specific period tracking app (advertisement). Four videos (two companies) promoted themselves as secure and private. Some focused on internal policies

Table 1: This table summarizes reproductive privacy advice on TikTok after the overturn of Roe v. Wade. We group advice by goals: tracking menstruation, communication, searching online for health information, and accessing reproductive healthcare. In parentheses, we show specific apps, programs, and services suggested. "No reason / general privacy" denotes that the connection between reproductive health and privacy was only a reproductive health-related hashtag, or a short statement like *How to protect your privacy after Roe v Wade....*

Advice	# videos
Advice about how (not) to track menstruation	
Delete all period tracking apps. Why?	12
→ Government access to data	
→ Data broker access to data	
→ Data mining	
→ Data leaks	
→ No reason / general privacy	
Delete a specific period tracking app. Why?	6
→ Government access to data (*Stardust*)	
→ Server is in Ireland—GDPR non-compliance (*Clue*)	
→ Data sharing with Meta (*Flo*)	
→ Do not trust the company (*Clue*)	
→ No reason / general privacy (*Apple health app*)	
Use a specific app. Why?	8
→ Servers in Europe (*Clue*)	
→ Don't sell data (*Clue, Flo*)	
→ No cloud storage/use (*Drip*)	
→ End-to-End Encrypted (*Apple health App*)	
→ No reason / general privacy (*Euki*)	
→ Non-privacy reasons (*Glow, Clue, Flo, Period Tracker by GP Apps*)	
Delete period-related data. Why?	6
→ Data leaks	
→ Selling data	
→ Government access to data	
→ No reason / general privacy	
Pen and paper tracking. Why?	8
→ Government access to data	
→ Selling data	
→ Data mining	
→ No reason / general privacy	
Advice about how to communicate about reproductive health	
Use encrypted communication. Why?	7
→ No reason / general privacy (*Signal, Protonmail/ temp email, Wire*)	
Don't communicate digitally at all. Why?	1
→ Data on phone	
Advice about searching online for reproductive health information	
Prevent online tracking with a specific browser or browser settings. Why?	6
→ Government surveillance (*DuckDuckGo, Incognito mode*)	
→ No reason / general privacy (*Tor, Brave, Firefox, Epic, Privacy Badger*)	
Change phone settings to prevent ad and app tracking. Why?	4
→ Reduce tracking	
→ No reason / general privacy	
Maintain a separate online identity. Why?	2
→ If getting an abortion	
→ No reason / general privacy	
Use VPN. Why?	3
→ Hide browsing history from ISP	
→ No reason / general privacy (*ExpressVPN*)	
External resources	10
Advice about how to access an abortion	
Get abortion medication by mail. Why?	5
→ No reason / general privacy	
Leave phone at home or use a burner phone. Why?	7
→ Protect location data	
→ Avoid data sharing with government	
→ No reason / general privacy	
Use a Faraday cage. Why?	1
→ Does not connect to outside signals	
Use cash or prepaid credit cards when paying for healthcare. Why?	5
→ Don't link identities	
→ No reason / general privacy	

about data sharing, omitting their legal obligation to respond to subpoenas and warrants. One company touted their commitment to not selling data: "*we are a safer alternative: try [company].... We will never ever sell your data*" (V72). Another explained their privacy policy: "*due to privacy concerns with Roe v. Wade, here's what we do to make sure your data is safe: we do not share or sell any personally identifiable information... although we do collect information like your name and address...only our employees and necessary vendors have access to that. Also, all of them signed confidentiality agreements, so they can't share it with third parties*" (V15).

In contrast, one period tracking company promoted their product by explaining that their use of encryption prevents access by law enforcement: "*our app generates a unique encryption key that only your phone knows. This private key—which we don't have access to—is the only thing that can connect your login information to your menstrual data. We don't have access to the data or save it anywhere. We don't even want to know it, so if the government subpoenas us, we won't be able to produce anything*" (V34). We observe that this design more completely protects users from remote data access by law enforcement and corporations.

TikTok advice: Track your period using pen and paper. Eight videos not only advised viewers to stop using period tracking apps, but to leverage *analog* tools to create offline menstruation calendars, to avoid menstrual data being mined, sold, or shared. For example, V6 demonstrated how to track one's cycle with a pen and paper: "*here's the tracker cycle*

in one minute....The first day of your cycle is when you begin bleeding... Let's say my period last for 5 days, so these days right here are your period length. Next, calculate your cycle length, which is the time in between periods" (V6).

Analog tracking is an example of asset-based [136] advice that fits the technical threat model, advocates for non-use of insecure or non-private technologies, and still enables users to achieve the main functional goal. However, because family and friends have been identified as potential adversaries [73], physical records of menstrual cycles may face physical security concerns. Additionally, analog tracking may require more effort to track, and especially to *predict* future periods.

TikTok advice: Delete period tracking data. In addition to advising viewers to use or not use period tracking apps, content creators also instructed viewers to delete historical data. Sometimes they gave no specific reason, and other times cited government access to historical data or the potential for data breaches because "*digital apps are often leaky*" (V32).

Several creators did not explicitly give reasons for deleting data. V85, about *Stardust*, advised: "*if you use this app, contact them, ask them to delete your data, and then delete the fucking app*" (V85). V8 even suggested altering data before deleting it, showing a screen recording of changing their data on a calendar. No video in our dataset had specific instructions on *how* to delete data from period tracking apps, e.g., through settings or contacting customer service, recalling findings about data deletion being convoluted in other contexts [94].

TikTok advice: Create fake menstrual data. In addition to advice focused on individual privacy, five videos suggested data poisoning by inputting false information into menstruation apps.V11 advised that "*if you don't get periods, install a period tracker. Flo is great way to track 'when I get coffee'*" (V11). V54 pointed to a Twitter post about being a "*cis man*" who inputs non-existent periods to a period tracking app to "*screw up data for any law enforcement agency that buys a database so they would have to waste a lot of resources cleaning it up*" (V54). It is unclear how effective this strategy would be in preventing prosecution.

4.2 Advice about avoiding tracking when seeking health information online

It is common to seek health information online [31], and in the post-Roe climate, private access to reliable online health information may be critical. As shown in Table 1, videos tailored general-purpose privacy strategies [100] to searching for reproductive health information. Though content creators gave examples and recommended specific technologies, they rarely precisely explained the threats addressed. This collection of strategies caters to protection against a corporate adversary rather than a government adversary (e.g., resetting the MAID reduces online ad tracking, and tightening app permissions reduces an app's collection of data), though the two are linked due to government access to corporate data through subpoena and other data sharing. No strategies addressed interpersonal threats from UI-bound attackers, such as intimate partners or family who have physical access to the device.

TikTok advice: Prevent online tracking with a specific browser or browser settings. Six videos recommended viewers use certain browser-based tools to reduce web tracking while searching for information about reproductive health. V70 recommended a host of tools for the "*privacy of your phone after Roe v. Wade...for the most browser privacy, use a browser like Tor, Epic, Firefox, or Brave*" (V70).

In addition to recommending certain browsers, two videos advocated for browser extensions, e.g., "*install a privacy-focused browser extension—it's not perfect but better than nothing*" (V14). V70 suggested "*something like Privacy Badger*" (V70). Others advised different browser settings or "*at least use incognito to look for abortion information*" (V60). V76 addressed the connection between browser data and subpoena, explaining that "*Google will respond to legit court orders with user data so your whole search history is up for grabs once an investigation starts. To avoid searches being recorded in your browsing history, sign out of Google or use a privacy-focused search engine like DuckDuckGo*" (V76). This advice collectively echos general-purpose privacy advice to reduce or prevent online tracking by third party trackers [100].

TikTok advice: Use a VPN. Three videos instructed viewers to use a VPN, indicating privacy from one's Internet Service Provider (ISP). V70, in a long list of recommendations to "*protect your phone data privacy after the overturn of Roe v. Wade*" (V70), suggested "*a VPN like Express VPN to hide your browsing history from Internet Service Provider*" (V70). V70 also advised a combination of VPN and temporary email when paying for reproductive care: "*Definitely first turn on your VPN, next create a new email account, and then after your appointment, immediately delete the email (or after you get receipts)*" (V70). V79 recommended viewers learn more about VPNs from the Digital Defense Fund: "*Visit DigitalDefensensefund.org/Abortion-Privacy because they have a lot more about how to use a VPN, which browsers to use, and how to avoid ad tracking*" (V79). While using a VPN is *generally* accepted as a tool to strengthen one's privacy and security, laypeople's mental models of VPNs are often incorrect [5], which could lead to an inappropriate sense of security. However, we note that a strength of these videos is that they recommend a VPN *in conjunction* with other privacy tools, giving complex privacy advice in a short video.

TikTok advice: Change phone settings. Four videos advised changing phone settings to reduce tracking. As part of their recommended strategies to "*protect your privacy on your phone after the overturn of Roe v. Wade*" (V70), V70 recommended viewers "*switch off mobile ad ID and location tracking*" (V70). Others advised changing app permissions. V84 showed viewers how to adjust iPhone app permissions: "*On an iPhone, open the settings app, scroll for a bit, go*

into privacy and security and click on tracking. If they're green, they have permission to track your activity. Go through all the apps and turn off permission for the ones that you don't want to track your activity" (V84). Prior work in mobile permissions indicates that apps are indeed often overpermissioned [35], and that users are overwhelmed with permission management [36]; we remark that the granularity of instruction in these videos may be effective technical instruction.

TikTok advice: Maintain a separate online identity. Five videos advised creating distinct online profiles to prevent pollution of users' primary online identity. V75 suggested that "*people seeking abortions... use an alias to set up other email and social media accounts for sensitive medical info*" (V75). V16 considered how peripheral technology use might lead to context collapse [69], recommending viewers "*try not to use apps like Vemmo, and be careful of wearable health devices like FitBit and Apple watch. Also be careful with digital voice assistants like Alexa and Portal, and cameras like Nest and Ring*" (V16). V16 connected this advice to reproductive health data through a caption invoking data privacy, and reproductive health-related hashtags.

TikTok advice: External resources for reproductive safety and privacy. Eight videos linked to external advice: notably, two linked to the Digital Defense Fund, and one to the Washington Post and the Electronic Frontier Foundation. V81 listed a broad set of threats to reproductive privacy, saying that the Digital Defense Fund can alleviate issues with "*your phone company hav[ing] copies of your texts or your browser history about your abortion..., whoever pays your phone bill seeing your messages..., protesters outside an abortion clinic [who] may violate your privacy..., tech companies like Google and Meta keeping data about your pregnancy/abortion..., someone who can steal, demand, or just access your phone seeing your texts or browser history*" (V81). V78 directs viewers to the Electronic Frontier Foundation, stating that "*to make sure your privacy is super protected, do everything they say*" (V78). As we discuss in Section 5, tailored external privacy resources created by experts may be a valuable tool in offsetting the limitations inherent in giving nuanced privacy advice in a short video.

TikTok advice: Use encrypted communication. Seven unique videos suggested using end-to-end encrypted communication apps such as Signal, Wire, and ProtonMail. Four videos recommended Signal: "*Here is some privacy advice for anyone who needs an abortion... your texts are not secure.... so instead use an encrypted messaging app, like Signal*" (V76).

Another video presents the case of a woman who was prosecuted for an illegal abortion, with her (unencrypted) text messages used as proof, highlighting how digital evidence of abortion-related communication led to prosecution. As a mitigation, the creator recommends "*looking at the Digital Defense Fund to learn how to protect your privacy—for example, secure your text messages, use Signal, etc*" (V69). One creator recommended Wire in addition to Signal, and advised disappearing messages: "*this is how to protect the privacy of your phone post-Roe....For sensitive texts, use an encrypted chat app like Signal or Wire and turn on disappearing messages*" (V70). V16, in a video tagged with privacy and reproductive-related hashtags, gave advice to use Proton Mail and Signal, instructing that "*there are some no-brainers you can follow to to protect your privacy and information*" (V16).

This advice reflects widespread advice to other vulnerable groups to use Signal, such as journalists and activists [27]. Prior work has found that advice to use Signal, while well-intentioned, can be harmful when it does not fit the target population, e.g., because simply *having* may raise suspicion [9], or because moving one's social network to a new app is a barrier to usage [3, 27], or because of usability issues or inaccurate mental models [12]. Indeed, creators did not explain the limitations and strengths of encrypted communications, protecting against threats from corporate data sharing but not interpersonal threats, which are particularly apparent in reproductive health [66, 73]. Additionally, V71 spread disinformation, telling viewers not to trust encrypted apps because law enforcement does not want companies to use "*military grade encryption*" and instead wants companies to provide access to "*secret keys*" to gain access to chats and information. Although encryption backdoors are a legitimate discussion in the technical and policy communities, V71's presentation of the issue does not reflect reality.

4.3 Advice about how to access an abortion

Finally, while much advice focused solely on digital privacy—keeping health information private in preparation for a potential pregnancy or abortion—other advice focused directly on how to maintain safety, privacy, and security while accessing an abortion (which may include miscarriage). Some advice connected existing strategies for abortion access to privacy, security, and safety; other advice applied privacy strategies typically used by activists [19, 27] to abortion access.

TikTok advice: Get abortion medication by mail. With rapidly changing reproductive health laws, five videos advised obtaining Mifepristone [91] via mail before pregnancy. Videos do not strongly link this advice to privacy, but imply that this strategy leverages the postal service to escape the complex privacy threats involved in purchasing medication in person. V19 warned viewers: "*I definitely recommend getting the abortion pill before you need it, because states are quickly restricting the fact that they can be mailed. These pills last 2 years*" (V19). Another recommended the US postal service's mail forwarding service to receive abortion pills in states where abortions are otherwise banned [4]: "*You can use mail forwarding to creatively get the abortion pill*" (V46).

[4] In May 2026, the US Supreme Court blocked an attempt to ban the mailing of one of the two medications used for at-home abortion, Mifepristone [49].

Virtual reproductive health clinics advertised their services as a response to privacy issues associated with in-person visits, consistent with findings from Song et al. [113]. As V30 (representing a company) advised, "*hey look, I can take the abortion pill from the comfort of my bed because I can get it mailed right to my house ... [company] currently ships the abortion pill to [7 states where abortion was not at the time severely restricted]*" (V30). One company touted shipping pills in unmarked envelopes with no return address in states with restricted reproductive care: "*If you need an abortion and can't go to a clinic, we can send you pills so you don't have to go in person*" (V51). We note that because these pills are ordered *online*, other privacy strategies are still necessary—and we remark that this is the *only* advice in our dataset that advocates for taking a previously offline activity online (here, for accessibility to those in restricted states).

TikTok advice: Leave phone at home or use a burner phone. Eight videos addressed the many ways smartphones track physical movement through the world—navigation apps, Bluetooth beacons, fitness tracking, etc—by advising viewers to leave their phones at home, turn them off, use a burner phone, or put their phone in a Faraday cage. Four creators advised not bringing one's personal smartphone to an abortion clinic: "*if you're going to an abortion clinic, you should turn off your phone or leave it at home*" (V14). Another advised viewers either to "*leave your phone at home... [or]...get another phone number*" (V16). Another creator further explained that "*experts advise the following for people who need a private abortion: Get a burner phone just for health stuff in order to protect your health information....*" (V75).

While a properly configured and separated burner phone can be a strong privacy strategy, it is both largely impractical and difficult to *completely* sever ties between the burner phone and one's identity, given SIM card registration and common requirements to tie new accounts to existing ones. It is unclear how fully decoupled a burner phone would need to be from one's identity to effectively address reproductive privacy threats.

TikTok advice: Use cash or prepaid cards for healthcare. Five content creators recommended cash or prepaid cards when paying for reproductive care; some explained that doing so would create a separation between payment history and identity. V76 stated that "*with abortion illegal or restricted in a lot of states, here are tips for seeking abortion care [...] when making online payments, the Digital Defense Fund recommends a gift card... because a gift card won't be connected to your name, phone number, or email*" (V76). In V78, the content creator recommended viewers "*buy a prepaid card and don't use a credit card because those can be linked back to you*" (V78) when purchasing reproductive care items. They also added links to privacy advice from the Washington Post and the Electronic Frontier Foundation as support.

TikTok advice: External resources for reproductive health. Two videos steered viewers towards external resources for health information, abortion funds, and medication. Some instructed viewers to search for certain organizations or websites, while others gave URLs and phone numbers directly. V26 dedicated their video to "*finding financial support for abortion from abortion funds*" (V26). They name six organizations that support people who need abortions, describing the target audience of each, e.g., " *mostly for people in the South*", and "*for Indigenous people only*" (V26). Others refer viewers to organizations (with URLs) for mail access to an abortion pill for early termination, as well as four other websites for access to abortion or abortion information, and two telephone hotlines. As we discuss in Section 5, links to external resources may be a strong strategy for overcoming the limitations of giving complex, actional, nuanced, and well-sourced privacy advice in short-form viral videos.

5 Discussion

Prior work states that in order to be useful, in addition to being comprehensible and technically sound, advice must be actionable [100, 103], and must be complete in addressing users' perceived threats in a crisis situation. Here, we synthesize lessons regarding the *actionability* and *completeness* of the security and privacy advice in our dataset of 92 TikTok videos released around the time of the overturn of Roe v. Wade. We emphasize that even technically sound advice may be impractical due to implementation challenges and ignorance of the user's context. Based on these lessons, we make recommendations for advice-givers—who may be content creators, journalists, advocacy organizations, social workers, etc.—social media platforms, and the security community both about applying general-purpose advice to a specific crisis or context, and leveraging existing domain-specific practices for privacy.

5.1 Practicality and actionability of advice

Social media is a powerful tool to quickly disseminate security and privacy advice [17, 19, 107]; however, it is challenging for TikTok creators to provide prioritized sound, actionable and complete advice (which experts also struggle with [85]), especially in short-form content. Additionally, providing security and privacy advice during a dynamic political landscape poses inherent challenges [109]. We present the following lessons about the actionability and practicality of reproductive privacy and security advice on social media.

The non-use of technology as a reproductive privacy strategy poses a burden on users. Much of the advice shared in our TikTok dataset advocated for avoiding technology, e.g., using cash to buy medication, pen and paper to track one's menstrual cycle, or leaving one's phone behind when traveling to healthcare appointments. While these strategies achieve the goal of privacy in some ways—by not self-creating digital records of health, purchases, or travel—they require the user to massively change their behavior and plan in a way that

may be new. Many people of reproductive age are digital natives [121,135], and may not have practiced analog navigation: looking up the address ahead of time, planning and memorizing or recording a route, and paying in cash for tolls, parking, or public transit. Additionally, advice for non-use generally constitutes *deficit-based* advice rather than *asset-based* advice, and is not aligned with HCI best practices [136].

General-purpose security and privacy advice often went unexplained. Security and privacy advice commonly found in other domains—like using a VPN, switching to an encrypted messenger, or using ad blockers—was often presented without explanation, echoing issues found in prior work with actionability of expert advice [103]. Most advice failed to explain why it was necessary (the threats it would mitigate) and how to set it up. Leaving this choice to users may burden them with making complex security decisions on their own, or can result in downloading unreliable and unsafe software.

Some privacy advice encourages isolationism. Some advice advocated for personal isolation when accessing illegal reproductive healthcare. While none of the videos in our data advocated for total isolationism or complete non-use of technology in all circumstances, videos rarely encouraged nuanced consideration of *who* to isolate from. Individual isolationist strategies may be effective for privacy (like avoiding disclosure to a spouse who might alert law enforcement [66]) but total isolationism is dangerous to one's physical and psychological well-being: Medical literature shows the importance of social support after surgical procedures like abortion and during and after pregnancy [6, 128]. Blanket advice to not use a certain technology or not communicate with certain people (without nuance and context) may lead to worse medical outcomes without, in some cases, changing the risk of prosecution or privacy violation.

5.2 Incomplete mental models of threats

Most videos in our dataset focused on a single privacy strategy. Through all 92 videos, 21 security and privacy strategies emerged, yet even collectively, the videos incompletely address the threats facing those seeking reproductive privacy in the US, are biased towards the non-use of technology, and lack guidance on informed and individualized privacy decision-making. As most advice-givers did not present themselves as computer security experts, it would be unrealistic to expect them to have a more comprehensive understanding of the threat and legal landscape, and to present it in an engaging short video. Below, we discuss lessons for the security and privacy community about the completeness of security and privacy advice on social media, towards advice that is *more complete* and better suited to its recipients.

Piecemeal advice to avoid technology incompletely addresses threats to reproductive privacy. To take one's reproductive health entirely off-grid would require not only tracking one's menstrual cycle on paper, but also, for example, purchasing menstrual and pregnancy supplies in person and in cash, without corporate rewards, traveling to and from stores and clinics without being recorded by any type of public surveillance or using a personally linked public transit card, etc. That is, it would be entirely impractical to take one's reproductive health completely off-grid, and thus recommendations to stop using technology in one specific way are, in isolation, likely ineffective.

Reproductive health companies presented themselves as secure and private, addressing threats to privacy from malware and insiders, but mostly not from law enforcement. In corroboration with prior work [113], we find that post Roe, companies communicated their stance on government data requests. As discussed in Section 4.1, companies highlighted their privacy practices—e.g., confidentiality agreements for employees—as sufficient protections. These public statements may help gain users' trust [10], but we observe that they often do not mention the (US) legal requirements to respond to government subpoenas.

As a collection, the advice has contradictions. Some content creators criticize certain apps, while others recommend the same app, resulting in contradictions in whether or not an app is safe to use. While it is out of scope to verify the safety of any individual app, we observe that these contradictions and imprecisions may be confusing. Additionally, it was sometimes hard to discern that videos were promotional posts because they were mostly posted from accounts of companies endorsing their products whose delivery resembled other content creators'. The posts were also not always tagged as promotional advertisements or marketing posts, though the US Federal Trade Commission [1] (and since late 2023 TikTok's content disclosure policy) require that partnerships and promotional content be labeled [122].

5.3 Comparison to advice for other groups

Security and privacy advice being repurposed or targeted at vulnerable populations during a crisis is a known phenomenon. Schmüser et al. found that much advice shared on Twitter during the Russia-Ukraine war was similar to general advice found in prior literature [100, 107]. Our findings also echo their observation—much of the "general" privacy and security advice discussed in Section 4 mirrored advice shared in other contexts, such as the 2020 Black Lives Matters protest in the US [19] and the Russian invasion of Ukraine [107], with all mentioning encrypted communication, ad blockers, privacy browsers, VPN, burner phones, and updating settings. The advice related to activism around turning off location sharing, disabling biometrics and not posting on social media were also mentioned in the advice provided to Sudanese activists [27]. This suggests that general purpose security and privacy advice remains constant across various contexts.

Prior work has noted context-specific security and privacy strategies emerging due to insufficient support from available technology and advice, e.g., during the Sudanese revolution [27] and the US Black Lives Matter protests [19]. Schmüser et al., in their study of advice during the Russian invasion of Ukraine, did not find non-general-purpose advice. This highlights the need for developing more context-specific advice in various situations, keeping in mind accurate threat models, capacity, knowledge, and circumstances of the users.

An additional problem often highlighted in prior work is advice prioritization [100, 101, 107]; similarly, much advice in our dataset was provided without stating how recipients can prioritize the advice they receive.

5.4 Recommendations

Finally, building on the lessons about advice actionability and completeness, we provide recommendations on how to *give better advice* during a crisis. We note that social media's algorithm shapes what content is visible to users. We also recognize a complex ecosystem involved in privacy advice on social media, and thus we urge social media platforms and security experts to share responsibility with content creators in giving privacy advice that is actionable, sound, and complete. The content creators in our dataset are mostly not experts in security and privacy, but they *are* experts on social media, and our recommendations respect their agency and their contributions to distributing security and privacy advice.

Recommendations for advice givers and content creators. It is an impractical and arduous task for content creators—especially those who are not privacy and security experts—to provide expert-level advice that is well researched and detailed, especially for a subject so complex and nuanced with a broad threat landscape. The use of short-format social media videos is also inherently limiting [80], leading to oversimplified or incomplete advice. Therefore, following the lead of a few videos in our dataset, we recommend advice givers always provide credible and verified *sources*, especially for complex security advice or decisions, e.g., by linking to credible sources like EFF [33], DDF [30], and Planned Parenthood [93]. Further, using a political event like this to promote software like period tracking apps trivializes the gravity of the situation and may mislead users into opting for software that does not actually protect them.

Recommendations for social media platforms. Social media platforms must ensure that promotional content is strictly labeled, as there is an inherent difference in motivation from a company that makes money by selling products, and an individual not connected to the company. Promotional posts that are provided as advice can mislead users. To alleviate this issue, we also recommend more carefully curating playlists of similar topics so that users can see multiple sources of advice at once.

Recommendations for the security community and experts. In our dataset, there were some healthcare and legal experts using TikTok to disseminate credible information. The security community can also use social media to communicate advice using more engaging, accessible content formats that reach and resonate with a much wider audience. Instead of expecting content creators to act more like expert users, experts can learn from content creators to produce content that can be reached by a wider audience. Also, the security community has made progress in providing actionable advice [103], and can further look into effective ways to promote sound and prioritized advice on social media.

Recommendations for adapting domain-specific strategies to privacy. Some advice was an application of reproductive health strategies (e.g., pen-and-paper period tracking) to privacy, rather than the application of privacy strategies to reproductive health. Indeed, general purpose privacy strategies often do not suit reproductive privacy threat contexts. For example, the advice to use E2EE communication suits someone who can trust those who can physically access their phone (spouse, friends, medical providers who may ask in the ER), but does not trust the platform on which they are communicating. However, the advice to use E2EE messaging fundamentally does not work for someone whose partner might turn them in for getting an abortion by providing screenshots from their phone [66]. Instead, in line with asset-based design [136], the use of community-driven, domain-oriented advice *as privacy strategies* may be a powerful way to curate context-sensitive privacy strategies that resonate with vulnerable users: leveraging practices that already exist in their community (such as analog menstruation tracking, or social networks already oriented towards reproductive care that might provide protection or aid in a time of need). When accounting for reproductive health, threats can arise interpersonally, and thus context is critical and was notably absent in much of the advice in our dataset. We therefore recommend exploring the adaptation of community practices to privacy rather than the other way around, as a way to give *actionable* and *community-oriented* privacy advice.

6 Conclusion

Following the US Supreme Court's decision to overturn Roe v. Wade, we analyzed advice on reproductive security and privacy on TikTok. While the advice is mostly technically sound, it lacks actionability and practicality, and the current advice landscape is neither sufficiently complete nor prioritized. Our results indicate, however, that with strategic advice curation based on expert recommendations, social media may be an effective medium for conveying helpful advice during geopolitical changes.

Acknowledgments

We are very grateful to our anonymous constructive and supportive SOUPS reviewers. This work was supported by the National Science Foundation under Grant No. 2445401.

References

[1] Disclosures 101 for Social Media Influencers. Federal Trade Commission, November 2019. https://www.ftc.gov/business-guidance/resources/disclosures-101-social-media-influencers, Accessed: 2025-01-22.

[2] AbortionFinder. State-by-State Guides to Abortion | U.S. AbortionLaws By Location, June 2026. https://www.abortionfinder.org/abortion-guides-by-state, Accessed: 2026-02-17.

[3] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 137–153. IEEE, 2017.

[4] Abigail RA Aiken, Kathleen Broussard, Dana M Johnson, and Elisa Padron. Motivations and Experiences of People Seeking Medication Abortion Online in the United States. *Perspectives on Sexual and Reproductive Health*, 50(4):157–163, 2018.

[5] Omer Akgul, Richard Roberts, Moses Namara, Dave Levin, and Michelle L Mazurek. Investigating influencer VPN ads on YouTube. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 876–892. IEEE, 2022.

[6] Anna L Altshuler, Alison Ojanen-Goldsmith, Paul D Blumenthal, and Lori R Freedman. "Going through it together": Being Accompanied by Loved Ones During Birth and Abortion. *Social Science & Medicine*, 284:114234, 2021.

[7] Katrin Amelang. (Not) Safe to Use: Insecurities in Everyday Data Practices with Period-Tracking Apps. In *New Perspectives in Critical Data Studies: The Ambivalences of Data Power*, pages 297–321. Springer, 2022.

[8] Morgan G Ames. Managing Mobile Multitasking: The Culture of iPhones on Stanford Campus. In *Proceedings of the 2013 conference on Computer supported cooperative work*, pages 1487–1498, 2013.

[9] Sarah Aoun. Working on the frontlines: Privacy and security with vulnerable populations. *USENIX Enigma 2023 (Talk)*, 2023.

[10] Oshrat Ayalon and Eran Toch. User-centered privacy-by-design: Evaluating the appropriateness of design prototypes. *International Journal of Human-Computer Studies*, 154:102641, 2021.

[11] Oshrat Ayalon, Dana Turjeman, and Elissa M Redmiles. Exploring Privacy and Incentives Considerations in Adoption of COVID-19 Contact Tracing Apps. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 517–534, 2023.

[12] Daniel V Bailey, Philipp Markert, and Adam J Aviv. "I have no idea what they're trying to accomplish:" Enthusiastic and Casual Signal Users' Understanding of Signal PINs. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 417–436, 2021.

[13] Michael Bailey, David Dittrich, Erin Kenneally, and Doug Maughan. The Menlo Report. *IEEE Security & Privacy*, 10(2):71–75, 2012.

[14] Catherine Barwulor, Allison McDonald, Eszter Hargittai, and Elissa M Redmiles. "Disadvantaged in the American-dominated internet": Sex, Work, and Technology. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2021.

[15] Eric PS Baumer, Phil Adams, Vera D Khovanskaya, Tony C Liao, Madeline E Smith, Victoria Schwanda Sosik, and Kaiton Williams. Limiting, Leaving, and (re)Lapsing: An Exploration of Facebook Non-Use Practices and Experiences. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 3257–3266, 2013.

[16] Emily Bazelon. Husband Sued Over His Ex-Wife's Abortion; Now Her Friends Are Suing Him. *The New York Times*, May 2023. https://www.nytimes.com/2023/05/04/us/texas-man-suing-ex-wife-abortion.html, Accessed: 2024-06-27.

[17] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. "Adulthood is trying each of the same six passwords that you use for everything": The Scarcity and Ambiguity of Security Advice on Social Media. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2), November 2022.

[18] Harry A. Blackmun (Judge) and Supreme Court of the United States (Author). U.S. Reports: Roe v. Wade, 410 U.S. 113 (1973) *Retrived from The Library of Congress*, [Periodical]. https://www.loc.gov/item/usrep410113, Accessed: 2026-17-06.

[19] Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. Understanding the Security and Privacy

Advice Given to Black Lives Matter Protesters. In *CHI 2021: ACM Conference on Human Factors in Computing Systems*, pages 1–18, 2021.

[20] Elizabeth Nolan Brown. Montana 'abortion trafficking' bill could criminalize crossing state lines for an abortion. *Reason Magazine*, February 2025. https://reason.com/2025/02/26/montana-abortion-trafficking-bill-could-criminalize-crossing-state-lines-for-an-abortion/, Accessed: 2025-12-06.

[21] Katharina Buchholz. The Rapid Rise of TikTok. *Statista*, October 2022. https://www.statista.com/chart/28412/social-media-users-by-network-amo/, Accessed: 2025-01-20.

[22] Amber M Buck and Devon F Ralston. I Didn't Sign Up for Your Research Study: The Ethics of Using "Public" Data. *Computers and Composition*, 61:102655, 2021.

[23] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 117–136, 2019.

[24] Jiaxun Cao, Hiba Laabadli, Chase H Mathis, Rebecca D Stern, and Pardis Emami-Naeini. "I Deleted It After the Overturn of Roe v. Wade"': Understanding Women's Privacy Concerns Toward Period-Tracking Apps in the Post Roe v. Wade Era. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, pages 1–22, 2024.

[25] Christine Chen, Nicola Dell, and Franziska Roesner. Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 89–104, 2019.

[26] Sophie Clark. Women Who Have Miscarriages Could Face Prosecution in West Virginia. Newsweek, 6 2025. https://www.newsweek.com/women-who-have-miscarriages-could-face-prosecution-west-virginia-2080231, Accessed 2025-06-05.

[27] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G Bardas. Defensive Technology Use by Political Activists During the Sudanese Revolution. In *2021 IEEE symposium on security and privacy (SP)*, pages 372–390. IEEE, 2021.

[28] Zehui Dai and Cory Higgs. Social Network and Semantic Analysis of Roe v. Wade's Reversal on Twitter. *Social Science Computer Review*, 42(1):186–200, 2024.

[29] Becca Damante and Kierra B Jones. A Year After the Supreme Court Overturned Roe v. Wade, Trends in State Abortion Laws Have Emerged. Center for American Progress, June 2023. https://www.americanprogress.org/article/a-year-after-the-supreme-court-overturned-roe-v-wade-trends-in-state-abortion-laws-have-emerged/, Accessed: 2024-09-27.

[30] DDF – Digital Defense Fund. Periods, Pregnancy, Abortion, and Your Digital Security, 2025. https://digitaldefensefund.org/ddf-slide-decks/periods-pregnancy-abortion-and-your-digital-security, Accessed: 2025-01-20.

[31] Munmun De Choudhury, Meredith Ringel Morris, and Ryen W White. Seeking and Sharing Health Information Online: Comparing Search Engines and Social Media. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 1365–1376, 2014.

[32] Mounika Deverashetti, K Ranjitha, and KV Pradeepthi. Security Analysis of Menstruation Cycle Tracking Applications Using Static, Dynamic and Machine Learning Techniques. *Journal of Information Security and Applications*, 67:103171, 2022.

[33] EFF – Electronic Frontier Foundation. Secure messaging scoreboard. https://www.eff.org/pages/secure-messaging-scorecard. Accessed: 2025-01-20.

[34] Sarah Emerson and Emily Baker-White. In A Post-Roe America, Googling "Abortion" Could Put You At Risk. Here's How To Protect Yourself. BuzzFeed News, May 2022. https://www.buzzfeednews.com/article/sarahemerson/abortion-digital-privacy-guide, Accessed: 2025-01-14.

[35] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. Android Permissions Demystified. In *Proceedings of the 18th ACM conference on Computer and Communications Security*, pages 627–638, 2011.

[36] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, pages 1–14, 2012.

[37] Gillian Fergie, Shona Hilton, and Kate Hunt. Young Adults' Experiences of Seeking Online Information About Diabetes and Mental Health in the Age of Social Media. *Health Expectations*, 19(6):1324–1335, 2016.

[38] Casey Fiesler, Michael Zimmer, Nicholas Proferes, Sarah Gilbert, and Naiyan Jones. Remember the Human: A Systematic Review of Ethical Considerations in Reddit Research. *Proc. ACM Hum.-Comput. Interact.*, 8(GROUP), February 2024.

[39] Leah R Fowler, Charlotte Gillard, and Stephanie R Morain. Readability and accessibility of terms of service and privacy policies for menstruation-tracking smartphone applications. *Health promotion practice*, 21(5):679–683, 2020.

[40] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW), December 2017.

[41] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. In *SOUPS 2019: Symposium on Usable Privacy and Security*, 2019.

[42] Flora Garamvolgyi. Why US women are deleting their period tracking apps. The Guardian, June 2022. https://www.theguardian.com/world/2022/jun/28/why-us-woman-are-deleting-their-period-tracking-apps, Accessed: 2024-09-02.

[43] Radhika Garg. An analysis of (non-)use practices and decisions of Internet of Things. In *Human-Computer Interaction–INTERACT 2019: 17th IFIP TC 13 International Conference, Paphos, Cyprus, September 2–6, 2019, Proceedings, Part IV 17*, pages 3–24. Springer, 2019.

[44] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a Low Profile? Technology, Risk and Privacy Among Undocumented Immigrants. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, pages 1–15, 2018.

[45] Vaughn Hamilton, Ananta Soneji, Allison Mcdonald, and Elissa M. Redmiles. "Nudes? Shouldn't I charge for these?": Motivations of New Sexual Content Creators on OnlyFans. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023.

[46] Ayako A Hasegawa, Naomi Yamashita, Tatsuya Mori, Daisuke Inoue, and Mitsuaki Akiyama. Understanding Non-Experts' Security-and Privacy-Related Questions on a Q&A Site. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 39–56, 2022.

[47] Kun He, Scott Eldridge, and Marcel Broersma. Tactics of Disconnection: How Netizens Navigate China's Censorship System. *Media and Communication*, 12:8670, 2024.

[48] Bryndl Hohmann-Marriott. Periods as Powerful Data: User Understandings of Menstrual App Data and Information. *New Media & Society*, 25(11):3028–3046, 2023.

[49] Amy Howe. Supreme Court allows for access to abortion pill by mail for now, May 2026. https://www.scotusblog.com/2026/05/court-allows-for-access-to-abortion-pill-by-mail-for-now/, Accessed: 2026-06-16.

[50] Amanda Lee Hughes and Leysia Palen. Twitter adoption and use in mass convergence and emergency events. *International Journal of Emergency Management*, 6(3-4):248–260, 2009.

[51] Zaidat Ibrahim, Pallavi Panchpor, Novia Nurain, and James Clawson. "Islamically, I am not on my period": A Study of Menstrual Tracking in Muslim Women in the US. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2024.

[52] Intersoft Consulting. General Data Protection Regulation (GDPR). https://gdpr-info.eu/. Accessed: 2025-01-20.

[53] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 327–346, Ottawa, July 2015. USENIX Association.

[54] Minal Jain and Pradeep Yammiyavar. Game based learning tool seeking peer support for empowering adolescent girls in rural Assam. In *Proceedings of the 14th International Conference on Interaction Design and Children*, pages 275–278, 2015.

[55] Jesus Jiménez. What is a Trigger Law? And Which States Have Them? The New York Times, May 2022. https://www.nytimes.com/2022/05/04/us/what-is-a-trigger-law-and-which-states-have-them.html, Accessed: 2025-04-11.

[56] Nadia Karizat, Nora McDonald, and Nazanin Andalibi. Laboring Towards Sociotechnical Reproductive Privacy in a Post-Roe United States: Identities, Technologies, and Actors Implicated in Reproductive Privacy. *Proc. ACM Hum.-Comput. Interact.*, 9(7), October 2025.

[57] Martin Kaste. Nebraska cops used Facebook messages to investigate an alleged illegal abortion. NPR, August 2022. https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion, Accessed: 2025-04-11.

[58] Leah R Koenig, Jennifer Ko, and Ushma D Upadhyay. Virtual Clinic Telehealth Abortion Services in the United States One Year After Dobbs: Landscape Review. *Journal of Medical Internet Research*, 26:e50749, 2024.

[59] Tadayoshi Kohno, Yasemin Acar, and Wulf Loh. Ethical Frameworks and Computer Security Trolley Problems: Foundations for Conversations. In *32nd USENIX Security Symposium (USENIX Security '23)*, pages 5145–5162, 2023.

[60] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW), December 2017.

[61] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. Co-designing Online Privacy-Related Games and Stories with Children. In *Proceedings of the 17th ACM Conference on Interaction Design and Children*, IDC '18, page 67–79, New York, NY, USA, 2018. Association for Computing Machinery.

[62] Hiba Laabadli, Yimeng Ma, Sofia Radkova, and Pardis Emami-Naeini. Exploring Security and Privacy Discourse on Twitter During theJustice Pour Nahel'Movement in France. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, pages 1–19, 2025.

[63] Johanna Levy and Nuria Romo-Avilés. "A good little tool to get to know yourself a bit better": A Qualitative Study on Users' Experiences of App-Supported Menstrual Tracking in Europe. *BMC Public Health*, 19:1–11, 2019.

[64] Library Of Congress. Constitution Annotated: Analysis and Interpretation of the U.S. Constitution, No Date. https://constitution.congress.gov/constitution/, Accessed: Jan 21, 2025.

[65] Erina L MacGeorge, Bo Feng, and Elizabeth R Thompson. "Good" and "Bad" Advice: How to Advise More Effectively. *Studies in Applied Interpersonal Communication*, 145, 2008.

[66] Doha Madani. Texas man sues ex-wife's friends, alleging they helped her get abortion pills in violation of state law. NBC News, March 2023. https://www.nbcnews.com/news/us-news/texas-man-sues-ex-wifes-friends-allegedly-helping-get-abortion-pills-v-rcna74541, Accessed: 2025-06-01.

[67] Isaac Maddow-Zimet and Candace Gibson. Despite Bans, Number of Abortions in the United States Increased in 2023. Guttmacher Institute, March 2024. https://www.guttmacher.org/2024/03/despite-bans-number-abortions-united-states-increased-2023, Accessed: 2025-04-11.

[68] Lisa Mekioussa Malki, Ina Kaleva, Dilisha Patel, Mark Warner, and Ruba Abu-Salma. Exploring Privacy Practices of Female mHealth Apps in a Post-Roe World. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–24, 2024.

[69] Alice E Marwick and Danah Boyd. I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience. *New media & society*, 13(1):114–133, 2011.

[70] Heather McCosker, Alan Barnard, and Rod Gerber. Undertaking sensitive research: Issues and strategies for meeting the safety needs of all participants. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, volume 2, 2001.

[71] Allison McDonald, Catherine Barwulor, Michelle L. Mazurek, Florian Schaub, and Elissa M. Redmiles. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 375–392. USENIX Association, August 2021.

[72] Nora McDonald and Nazanin Andalibi. "I Did Watch 'The Handmaid's Tale'": Threat Modeling Privacy Post-roe in the United States. *ACM Transactions on Computer-Human Interaction*, 30(4):1–34, 2023.

[73] Nora McDonald, Alan Luo, Phoebe Moh, Michelle L Mazurek, and Nazanin Andalibi. Threat Modeling Healthcare Privacy in the United States. *ACM Transactions on Computer-Human Interaction*, 2024.

[74] Maryam Mehrnezhad and Teresa Almeida. "My sex-related data is more sensitive than my financial data and I want the same level of security and privacy": User Risk Perceptions and Protective Actions in Female-oriented Technologies. In *Proceedings of the 2023 European Symposium on Usable Security*, pages 1–14, 2023.

[75] Maryam Mehrnezhad, Laura Shipp, Teresa Almeida, and Ehsan Toreini. Vision: Too Little Too Late? Do the Risks of FemTech Already Outweigh the Benefits? In *Proceedings of the 2022 European Symposium on Usable Security*, pages 145–150, 2022.

[76] Tamir Mendel. Social Help: Developing Methods to Support Older Adults in Mobile Privacy and Security. In *UbiComp/ISWC 2019: ACM International Joint Conference on Pervasive and Ubiquitous Computing and ACM International Symposium on Wearable Computers*, 2019.

[77] Helena M. Mentis, Galina Madjaroff, and Aaron K. Massey. Upside and Downside Risk in Online Security for Older Adults with Mild Cognitive Impairment. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–13, New York, NY, USA, 2019. Association for Computing Machinery.

[78] Angela Molem, Stephann Makri, and Dana Mckay. Keepin'it Reel: Investigating How Short Videos on TikTok and Instagram Reels Influence View Change. In *Proceedings of the 2024 Conference on Human Information Interaction and Retrieval*, pages 317–327, 2024.

[79] Diana P Moniz, Maryam Mehrnezhad, and Teresa Almeida. Intimate data: Exploring perceptions of privacy and privacy-seeking behaviors through the story completion method. In *IFIP Conference on Human-Computer Interaction*, pages 533–543. Springer, 2023.

[80] Lisa Montenegro. The rise of short-form video: Tiktok is changing the game. Forbes Agency Council, April 2022. https://www.forbes.com/councils/forbesagencycouncil/2021/08/27/the-rise-of-short-form-video-tiktok-is-changing-the-game/, Accessed: 2025-01-20.

[81] Matt Motta, Yuning Liu, and Amanda Yarnell. "Influencing the influencers:" A field experimental approach to promoting effective mental health communication on TikTok. *Scientific reports*, 14(1):5864, 2024.

[82] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya. In *S&P 2022: IEEE Symposium on Security and Privacy*, 5 2022.

[83] Savanthi Murthy, Karthik S. Bhat, Sauvik Das, and Neha Kumar. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. In *CHI 2021: ACM Conference on Human Factors in Computing Systems*, 2021.

[84] Elizabeth Nash and Isabel Guarnieri. 13 States Have Abortion Trigger Bans—Here's What Happens When Roe Is Overturned. Guttmacher Institute, June 2022. https://www.guttmacher.org/article/2022/06/13-states-have-abortion-trigger-bans-heres-what-happens-when-roe-overturned, Accessed: 2025-04-11.

[85] Lorenzo Neil, Harshini Sri Ramulu, Yasemin Acar, and Bradley Reaves. "Who comes up with this stuff?" Interviewing Authors to Understand How They Produce Security Advice. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 283–299, 2023.

[86] Nidhi Nellore and Michael Zimmer. Femtech Data Privacy post-Dobbs: A Preliminary Analysis of User Reactions. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing*, pages 226–228, 2023.

[87] Borke Obada-Obieh, Yue Huang, Lucrezia Spagnolo, and Konstantin Beznosov. SoK: The Dual Nature of Technology in Sexual Abuse. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 2320–2343. IEEE, 2022.

[88] Kentrell Owens, Anita Alem, Franziska Roesner, and Tadayoshi Kohno. Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives. In *31st USENIX Security Symposium (USENIX Security 22)*, Boston, MA, August 2022. USENIX Association.

[89] Kentrell Owens, Camille Cobb, and Lorrie Cranor. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[90] Leysia Palen and Kenneth M Anderson. Crisis informatics—new data for extraordinary times. *Science*, 353(6296):224–225, 2016.

[91] Planned Parenthood. The facts on mifepristone. https://www.plannedparenthood.org/uploads/filer_public/42/8a/428ab2ad-3798-4e3d-8a9f-213203f0af65/191011-the-facts-on-mifepristone-d01.pdf. Accessed: 2025-06-01.

[92] Planned Parenthood Action Fund. Roe v. wade overturned: How the supreme court let politicians outlaw abortion. https://www.plannedparenthoodaction.org/issues/abortion/roe-v-wade#effect. Accessed: 2025-01-20.

[93] Planned Parenthood Hudson Peconic, Inc. Security information. https://www.plannedparenthood.org/planned-parenthood-hudson-peconic/patient-resources/security-information. Accessed: 2025-01-20.

[94] Amogh Pradeep, Johanna Gunawan, Alvaro Feal, David Choffnes, and Woodrow Hartzog. Gig Work at What Cost?: Exploring Privacy Risks of Gig Work Platform Participation in the U.S. In *Proceedings of 25th Privacy Enhancing Technologies Symposium*, PoPETS'25. Privacy Enhancing Technologies Symposium, 2025.

[95] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. "Woe is me:" Examining Older Adults' Perceptions of Privacy. In *CHI EA 2019: Extended Abstracts of ACM Conference on Human Factors in Computing Systems*, 2019.

[96] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. "Warn Them" or "Just Block Them"?: Investigating Privacy Concerns Among Older and Working Age Adults. *Proceedings on Privacy Enhancing Technologies*, 2021.

[97] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. Why Older Adults (Don't) Use Password Managers. In *Security 2021: USENIX Security Symposium*, 2021.

[98] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 666–677, New York, NY, USA, 2016. Association for Computing Machinery.

[99] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 272–288, 2016.

[100] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 89–108, 2020.

[101] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy*, 15(5):55–64, 2017.

[102] Celia Rosas. The future is FemTech: Privacy and data security issues surrounding FemTech applications. *Hastings Bus. LJ*, 15:319, 2019.

[103] Anna Lena Rotthaler, Harshini Sri Ramulu, Lucy Simko, Sascha Fahl, and Yasemin Acar. "It's time. Time for digital security.": An End User Study on Actionable Security and Privacy Advice. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 100–100. IEEE Computer Society, 2024.

[104] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 'Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *SOUPS 2018: Symposium on Usable Privacy and Security*, 2018.

[105] Devansh Saxena, Patrick Skeba, Shion Guha, and Eric PS Baumer. Methods for generating typologies of non/use. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW1):1–26, 2020.

[106] Anastasia Schaadhardt, Yue Fu, Cory Gennari Pratt, and Wanda Pratt. "Laughing so I don't cry": How TikTok users employ humor and compassion to connect around psychiatric hospitalization. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2023.

[107] Juliane Schmüser, Harshini Sri Ramulu, Noah Wöhler, Christian Stransky, Felix Bensmann, Dimitar Dimitrov, Sebastian Schellhammer, Dominik Wermke, Stefan Dietze, Yasemin Acar, and Sascha Fahl. Analyzing Security and Privacy Advice During the 2022 Russian Invasion of Ukraine on Twitter. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2024.

[108] Laura Shipp and Jorge Blasco. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proceedings on Privacy Enhancing Technologies*, 2020.

[109] Lucy Simko. *Humans and Vulnerability During Times of Change: Computer Security Needs, Practices, Challenges, and Opportunities*. University of Washington, 2022.

[110] Lucy Simko, Adryana Hutchinson, Evan Fries, Alvin Isaac, Micah Sherr, and Adam J Aviv. "Modern Problems Require Modern Solutions": Community-developed techniques for online exam proctoring evasion. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security*, 2024.

[111] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer Security and Privacy for Refugees in the United States. In *2018 IEEE symposium on security and privacy (SP)*, pages 409–423. IEEE, 2018.

[112] Ananta Soneji, Vaughn Hamilton, Adam Doupé, Allison McDonald, and Elissa M. Redmiles. "I feel physically safe but not politically safe": Understanding the Digital Threats and Safety Practices of OnlyFans Creators. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 1–18, Philadelphia, PA, August 2024. USENIX Association.

[113] Qiurong Song, Rie Helene Hernandez, Yubo Kou, and Xinning Gui. "Our Users' Privacy is Paramount to Us": A Discourse Analysis of How Period and Fertility Tracking App Companies Address the Roe v Wade Overturn. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–21, 2024.

[114] Qiurong Song, Renkai Ma, Yubo Kou, and Xinning Gui. Collective Privacy Sensemaking on Social Media about Period and Fertility Tracking post Roe v. Wade. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW1):1–35, 2024.

[115] Aparna Sridhar. Spontaneous abortion. MSD Manual, October 2023. https://www.msdmanuals.com/professional/gynecology-and-obstetrics/early-pregnancy-disorders/spontaneous-abortion, Accessed: 2025-06-01.

[116] Statista. TikTok: Distribution of Global Audiences 2024, by Age and Gender, May 2024. https://www.statista.com/statistics/1299771/tiktok-global-user-age-distribution/, Accessed: 2024-08-19.

[117] Sophie Stephenson, Christopher Nathaniel Page, Miranda Wei, Apu Kapadia, and Franziska Roesner. Sharenting on TikTok: Exploring Parental Sharing Behaviors and the Discourse Around Children's Online Privacy. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2024.

[118] Cora Sula, Elizabeth Gorman, Kaitlyn Wei, Phoebe Moh, Nora McDonald, and Lucy Simko. From A to Zines: Narrative Threat Modeling in U.S. Reproductive Health Media. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*, CHI '26, New York, NY, USA, 2026. Association for Computing Machinery.

[119] Yunpeng Sun, Ruoya Jia, Asif Razzaq, and Qun Bao. Social network platforms and climate change in China: Evidence from TikTok. *Technological Forecasting and Social Change*, 200:123197, 2024.

[120] Supreme Court of the United States. Thomas E. Dobbs, State Health Officer of the Mississippi Department of Health, et al., Petitioners v. Jackson Women's Health Organization et al. Opinion of the Court, June 2022. https://www.supremecourt.gov/opinions/21pdf/19-1392_6j37.pdf, No. 19–1392. Decided June 24, 2022. Accessed: 2025-01-20.

[121] TechTarget. Digital native. https://www.techtarget.com/whatis/definition/digital-native, 6 2020. Accessed: 2025-01-20.

[122] TikTok. Promoting a brand, product, or service. https://support.tiktok.com/en/business-and-creator/creator-and-business-accounts/promoting-a-brand-product-or-service. Accessed: 2024-09-02.

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

[124] Mindy Tran, Collins W Munyendo, Harshini Sri Ramulu, Rachel Gonzalez Rodriguez, Luisa Ball Schnell, Cora Sula, Lucy Simko, and Yasemin Acar. Security, Privacy, and Data-sharing Trade-offs When Moving to the United States: Insights from a Qualitative Study. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 4–4. IEEE Computer Society, 2023.

[125] Anupriya Tuli, Surbhi Singh, Rikita Narula, Neha Kumar, and Pushpendra Singh. Rethinking menstrual trackers towards period-positive ecologies. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–20, 2022.

[126] Warda Usman and Daniel Zappala. SoK: A framework and guide for human-centered threat modeling in security and privacy research. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 2697–2715. IEEE, 2025.

[127] Danny Valdez, Lucrecia Mena-Meléndez, Brandon L Crawford, Akshat Arvind, and Kristen N Jozkowski. Online Social Media Reactions to the Overturn of Roe v. Wade: Public Health Implications and Policy Insights. *Sexuality Research and Social Policy*, 21(2):616–631, 2024.

[128] Mariana B Veiga, Melanie Lam, Carla Gemeinhardt, Edwina Houlihan, Brian P Fitzsimmons, and Zoë G Hodgson. Social support in the post-abortion recovery room: evidence from patients, support persons and

nurses in a Vancouver clinic. *Contraception*, 83(3):268–273, 2011.

[129] Sarah Vieweg, Amanda L Hughes, Kate Starbird, and Leysia Palen. Microblogging During Two Natural Hazards Events: What Twitter May Contribute to Situational Awareness. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1079–1088, 2010.

[130] Anna Claire Vollers. 200+ women faced criminal charges over pregnancy in year after dobbs, report finds. Missouri Independent, October 2024. https://stateline.org/2024/10/01/200-women-faced-criminal-charges-over-pregnancy-in-year-after-dobbs-report-finds/, Accessed: 2025-04-11.

[131] Miranda Wei, Sunny Consolvo, Patrick Gage Kelley, Tadayoshi Kohno, Tara Matthews, Sarah Meiklejohn, Franziska Roesner, Renee Shelby, Kurt Thomas, and Rebecca Umbach. Understanding Help-Seeking and Help-Giving on Social Media for Image-Based Sexual Abuse. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 4391–4408, Philadelphia, PA, August 2024. USENIX Association.

[132] Miranda Wei, Sunny Consolvo, Patrick Gage Kelley, Tadayoshi Kohno, Franziska Roesner, and Kurt Thomas. "There's so much responsibility on users right now:" Expert Advice for Staying Safer From Hate and Harassment. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2023.

[133] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. Anti-Privacy and Anti-Security Advice on TikTok: Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships. In *Proceedings of the Eighteenth USENIX Conference on Usable Privacy and Security*, pages 447–462, 2022.

[134] Rosemary Westwood. After historic indictment, doctors will keep mailing abortion pills over state lines. NPR Heard on Morning Edition, March 2025. https://www.npr.org/sections/shots-health-news/2025/03/19/nx-s1-5312115/margaret-carpenter-indictment-telemedicine-abortion-louisiana-mail-mifepristone-misoprostol, Accessed: 2025-11-04.

[135] WHO – World Health Organization. Women of reproductive age (15-49 years) population (thousands). https://platform.who.int/data/maternal-newborn-child-adolescent-ageing/indicator-explorer-new/mca/women-of-reproductive-age-(15-49-years)-population-(thousands). Accessed: 2025-01-20.

[136] Marisol Wong-Villacres, Aakash Gautam, Wendy Roldan, Lucy Pei, Jessa Dickinson, Azra Ismail, Betsy DiSalvo, Neha Kumar, Tammy Clegg, Sheena Erete, et al. From needs to strengths: Operationalizing an assets-based design of technology. In *Companion Publication of the 2020 Conference on Computer Supported Cooperative Work and Social Computing*, pages 527–535, 2020.

[137] World Health Organization. Adolescent pregnancy, April 2024. https://www.who.int/news-room/fact-sheets/detail/adolescent-pregnancy, Accessed: 2024-12-14.

[138] Michael Zimmer. "But the data is already public": On the Ethics of Research in Facebook. In *The ethics of Information Technologies*, pages 229–241. Routledge, 2020.

A How we altered quotes

In line with best practices for research on public social media [22, 38, 106, 110, 117, 133, 138], we changed each quote so that it retains the tone and meaning of the original quote, but cannot be followed back to the original creator as best as we can tell. To alter quotes, one researcher followed the following rules (following the lead of recent prior work on Tiktok data [110]):

- For all quotes: Remove any potentially identifying information about the creator (e.g., first name, location, etc) (there was none)
- For quotes five words or less: the researcher used their discretion (and ended up changing none).
- For quotes from a corporate account that were self-promotion: the researcher did not change these, as they are not personal.
- For all other quotes: Alter the quote by doing the following until we expect it would not be found through automated search in a database of original transcripts
  - changing *sentence structure*,
  - swapping out synonyms,
  - retaining tone, sentiment, and some slang
- Another researcher checked the altered quotes for tone, sentiment, and slang retention, as well as sufficient alteration.

B Codebook

Code	Sub-code
Recommended (digital) S&P Practices	Use a secondary email, Use a secondary phone number, Use a temporary email, Turn off the device if going to a place with higher surveillance, Use a VPN, Use a private web browser, Use encrypted emails, Use E2EE messaging, Use private browser on mobile & desktop, Read privacy terms & conditions, Don't text friends about your abortion, Privacy extension on browser
Recommended Privacy Tools	**VPN:** Express VPN, **Private Browsing:** DuckDuck Go, Brave, Firefox, Incognito mode, TOR, Epic, **Secondary phone number:** Burner phone, **Encrypted email**: Proton Mail, **Encrypted messaging:** Signal, Wire
Data Sharing	Get consent before sharing personal information of others (e.g., pictures), Use codewords or special phrases to mask sensitive communication, Limit personal data sharing, Stop sharing on social media
Seeking Advice	Follow advocacy groups, Look at articles (media), Look at resources
Phone Settings	Limit/ stop location sharing for period tracking apps, Beware of sharing location data (e.g., when you visit abortion clinics), Look at privacy settings for apps and accounts, Use passcodes instead of fingerprints/ face identification, Web search history, Phone records being stored, Disable ad IDs, Turn off location on phone, Turn on disappearing messages
Misinformation	Beware of bad advice, Beware of crisis pregnancy centers, Debunking misinformation
Data Handling & Storage	Delete period-related data, Do not store backups of period-related data in the cloud, Use pseudonymous on apps, Pseudonyms can be tracked back to you, Data brokers selling location data, Apps selling period data, Create incorrect data on purpose in period apps
Helpline & Support	Helpline number for medical advice, Helpline number for legal advice, Helpline for self-managed abortion, Helpline for miscarriage, Women's healthcare, Use/ donate to abortion funds, Do not donate to Planned Parenthood
Real Life Advice	Avoid states, Where to get pill (abortion), Go analog (pen and paper), Use virtual/ digital calendar, Use spreadsheets/ excel, Buy pregnancy tests in bulk, Do not mention to anyone if you may be pregnant, Do not tell anyone if you're getting an abortion, Use cash or pre-paid gift card for abortions/ repro health-related, Leave your partner who supports abortion ban, Leave your phone at home, Do not use loyal programs/ reward cards, Use mail forwarding, When going to abortion/repro health appointments turn on airplane mode with Bluetooth off, Beware of violence/ extremists when going to a clinic, Protest tips for what to do with technology to maintain your privacy and security
Bad Advice	"Do not get pregnant" advice, Do not have sex
Disruption Advice	Men download period apps, Download multiple period trackers and add wrong period info
Government & Legal	Need data privacy regulations, Need governments to pass laws to protect abortion rights, Explaining Roe Vs Wade and privacy, Prevent companies from selling private information, Explaining laws related to medical care that also apply to reproductive health, Laws regarding minors and abortion/ medical, Subpoenas/ warrants, **Know your legal rights advice:** Police need a warrant for your phone, Know that HIPAA does not apply to period tracking apps, Illegal to provide medical advice
Period Tracking Apps: Pros	App data storage location, Data sharing, Transparency about data sharing, Location sharing, Option to anonymize/pseudonymize data, Data is encrypted, No account needed, Won't sell data, Track cycle through body symptoms (not predicted algorithm)
Recommended Period Trackers	Drip, Euki, Apple health app, Stardust, Clue, Period tracker by GP apps, Glow, Flo, Period (app)
Issues Period tracking apps	Collect personal/ sensitive information, Share data with a third party, Non-transparent about sharing data, Inconsistencies between privacy policies and practice, Data not protected by HIPAA can be sold/given to third parties and law enforcement etc. Read private policies, Data being leaked, Cloud-based storage
Period tracker/ Apps to avoid	Flo, Apple health app, Clue, Stardust
Promotional content	Online abortions provider, Period tracking apps, Period product company
Tracking and Surveillance	Beware of leaving a digital footprint, Beware of leaving your search history, Beware of the data you are not willingly sharing, Beware of third parties such as people in your life, Beware of calls emails
Unsafe and self-managed abortions/ practices	At-home abortions, Unsanitary conditions, Unsafe or illegal procedures, How to get abortion pills online, Warns about unsafe abortions, Inducing abortions, Beware of fake clinics
Repercussions of criminalizing abortions	Trauma, Cases of abuse, No access to safe healthcare post-abortion, No access to safe legal care post-abortion, Lack of support for marginalized populations, Legal repercussions (fees, imprisonment), End/ limitation to the right to privacy/ lack of protection for medical records (hiring managers can see), Affects low income people/ same-sex marriages/ civil rights, financial harms
Advice Source	Media, News agency, Individuals (unkown source), NGO (reproductive rights organization/ human rights organization etc.), Lawyer, Academic, HCP (Health Care Providers)