Threat Modeling Healthcare Privacy in the United States

NORA MCDONALD, George Mason University, USA
ALAN LUO, University of Maryland, USA
PHOEBE MOH, University of Maryland, USA
MICHELLE L. MAZUREK, University of Maryland, USA
NAZANIN ANDALIBI, University of Michigan, USA

The landscape of digital privacy risks faced by individuals seeking abortions has grown increasingly complex following the overturn of Roe v. Wade. Reproductive healthcare providers are uniquely positioned to offer critical privacy guidance. We conducted interviews with 22 reproductive healthcare providers across the U.S. to explore their perceptions of privacy threats for abortion-seeking patients and the types of guidance they provide. Our findings show that providers are most concerned about privacy risks for vulnerable patients—minors, individuals seeking gender-affirming care, and those in abusive relationships—particularly regarding information that could be intercepted by people close to them, such as partners or relatives. However, providers generally do not perceive government surveillance or hostile actors as major threats to abortion-seeking patients. We conclude with an updated notion of *informed consent* and preliminary recommendations for ways healthcare providers can revise their threat models to better support the privacy of abortion-seeking patients.

CCS Concepts: • **Human-centered computing → Human computer interaction (HCI)**; **Empirical studies in HCI**; • **Security and privacy → Social aspects of security and privacy**;

Additional Key Words and Phrases: Reproductive health, reproductive justice, healthcare, privacy, vulnerable populations

1 INTRODUCTION

In *When Abortion Was a Crime*, Leslie J. Reagan writes that, "it would have been virtually impossible for the state to enforce criminal abortion laws without the cooperation of physicians," and that the "medical profession and its institutions acted as an arm of the state" by observing and reporting illegal behavior [102]. Abortion is once again a crime in many states in the U.S., but enforcement of abortion restrictions and bans in today's digital landscape takes on far more expansive dimensions, encompassing devices, social media and third-party data, and electronic health records (EHRs). Hostile healthcare providers[1] reporting on patients they suspect of exposing a fetus to

[1]Unless otherwise specified, "healthcare providers" refers to individuals who work in healthcare settings and includes those who provide medical or other care (e.g., nurse, doctor, social workers) who have access to EHRs. We detail the titles and roles of the "*reproductive* health providers" we interviewed in the methods section. Sometimes we refer to providers of other services like Internet, counseling, legal, etc. When we do, we specify their roles.

Authors' addresses: Nora McDonald, nmcdona4@gmu.edu, George Mason University, 435 Research Hall, Fairfax, Virginia, USA, 22030; Alan Luo, alanfluo@umd.edu, University of Maryland, 5112 Iribe Center, College Park, Maryland, USA, 20742; Phoebe Moh, pmoh@umd.edu, University of Maryland, 5112 Iribe Center, College Park, Maryland, USA, 20742; Michelle L. Mazurek, mmazurek@umd.edu, University of Maryland, 5236 Iribe Center, College Park, Maryland, USA, 20742; Nazanin Andalibi, andalibi@umich.edu, University of Michigan, 105 S State St., Ann Arbor, Michigan, USA, 48109.

ACM 1557-7325/2024/11-ART
https://doi.org/10.1145/3704634

harm [64, 71], or of an abortion [59, 106] has long been a concern. Before the Dobbs decision,[2] reproductive justice advocates have noted an alarming increase in the number of people capable of pregnancy who have been subject to criminal arrest from 2006 to June 2022 [71]. These cases were often instigated by healthcare providers, but new laws seem to incentivize reporting by family members suspected or known to have had an abortion [29, 95], and digital access seems to provide new avenues for prosecution.

First, let's examine the providers in this realm. Although reproductive clinics—and those that fund them [116]—may limit the flow of patient reproductive data, they face the threat of having to surrender protected health information (PHI) to authorities, including states with more restrictive abortion laws [4, 75, 78, 106]. While healthcare providers may be subject to investigation and subpoenas for their records [28, 106, 138], hostile providers may report patients suspected of seeking abortions to the police [59]. It is also now possible for them to gain access to data shared on Health Insurance Portability and Accountability Act (HIPAA)-protected EHRs [106, 143]. State attorneys general are increasingly seeking access to the medical records of individuals pursuing out-of-state abortions [4, 78].

Second, reproductive healthcare patients are also vulnerable to investigation of their social media accounts and other third-party data instigated by hostile healthcare providers *and* people close to them who may take on a vigilante role [112, 124]. There is the risk that activities conducted on personal devices—browsing [112, 124], purchases [37], location [45, 131], messages exchanged with friends or family [43, 70]—can be used in prosecution. Authorities have shown a willingness to issue warrants for records related to reproductive health crimes to social media companies [25, 70, 98], and they also find ways to access individuals' devices and data with relative ease [112].

Despite protections theoretically offered by the Health Insurance Portability and Accountability Act (HIPAA), gaps remain in safeguarding reproductive health information. For instance, there exist threats from apps that collect data about patients' health that claim to be privacy-protective, including from EHRs [1]. These apps may be intercepted by hostile healthcare providers —who may feel empowered to report patients—or by healthcare portals or other health related apps not bound by HIPAA [35, 41, 105]. According to the U.S. Department of Health and Human Services (HHS), while apps provided by healthcare providers may be protected by HIPAA, healthcare related data captured outside of medical portals are not [35, 59, 105, 107], nor are pharmacy data [63, 129]. What's more, companies that provide healthcare portals also reserve the right to sell patient health records for advertising, and some claim that they are not constrained by HIPAA [53]. These companies may also claim these data are not identifiable, but examples abound of supposedly deidentified data being reidentified [94, 113, 137].

While HIPAA may offer *some* protection for institutions aiming to safeguard patient data, warrants can permit the disclosure of these data [104]. Once seen as an impenetrable shield, HIPAA now resembles a loose curtain over patient privacy, as laws are not only *written* but also *interpreted* through litigation and prosecution. Consequently, we are still learning what HIPAA does and does not protect, particularly as states seek to extract information for enforcement purposes. No single legal determination can be seen as definitive in the face of aggressive and creative tactics used to exploit pregnant people's personal information to prevent or punish abortion.

It would thus appear that the vectors of privacy leakage and prosecutorial threat have broadened to include several key groups: **Unwitting healthcare providers:** Medical records can travel across state lines into the hands of hostile healthcare providers in states where abortion is illegal. These providers may feel empowered to report patients who receive abortions [74, 143].[3] **Patients:** Their records may be seized across state lines [4, 75, 78]. **Friends, family, and partners**: These individuals may learn about abortions through various means [84, 95, 115, 128]. **State authorities:** These officials may gain knowledge of suspected abortions from healthcare

[2]In Dobbs v Jackson Women's Health Organization (2022) the Supreme Court of the United States ruled that the U.S. Constitution does not protect the right to an abortion, effectively overruling the landmark cases Roe v. Wade (1973) and Planned Parenthood v. Casey (1992). This decision returned to states the power to regulate abortion.

[3]This also includes healthcare providers whose EHRs are subpoenaed by law enforcement.

providers [43, 59, 112, 124] or have access to patients' search histories [111], social media [70, 81, 98], online reproductive health activities [63, 72], or visits to clinics [24, 45, 131].

Post-Roe, prohibitions seem increasingly formidable because the panopticon[4] continually broadens the "vast attack surface for surveillance" [35]. Taken together, abortion-seeking individuals face digital privacy risks from all sides: EHRs, social platforms, third parties. Some of this risk quite literally comes from "inside the house"—i.e., one's own device or those of one's intimate circle—giving law enforcement a sightline into evidence that can be used to prosecute abortions. Still, reproductive healthcare providers may be in a position to help.

Reproductive care clinics take seriously their role in protecting patients from EHR-based threats from authorities seeking records and threats from within their walls—other patients, or individuals patients bring to the clinic. However, current and emerging threats to reproductive health freedoms require that healthcare providers be equipped to offer their patients more holistic guidance that take into account the vast surface area of threat, including patients' own devices, as well as EHR that travels outside their walls. This sort of competence is not part of their professional training, which means that protocols are only now being developed or improvised (if at all) in response to practical, urgent need. Consequently, we know very little about the practices reproductive healthcare providers are following, beyond standard patient confidentiality, in their efforts to support patient privacy and care post-Roe. This is important as all those well acquainted with the risks and structural challenges faced by vulnerable groups are ideally positioned to provide privacy guidance [80, 89, 119].

This research explores, at a high level, how U.S. reproductive healthcare providers thinking about privacy for abortion-seekers amid rapidly changing and increasing legal threats to bodily autonomy. Specifically, it examines the risks providers are concerned about, the practices they employ, and the types of privacy guidance they currently offer—or wish to offer—to their patients. To address these questions, we conducted 22 interviews with reproductive healthcare providers (referred to as "providers" in our findings) across the U.S.

We find that the reproductive healthcare providers we spoke with are primarily concerned about threats arising from the flow of information that emanates from their practices—specifically, conversations and written records exchanged between patients and providers through electronic communications that could be intercepted by patients' partners, other family members, or close associates. These concerns are mostly focused on patients whom they consider most vulnerable—minors, individuals seeking gender-affirming care, and those in abusive relationships—who are seeking legal reproductive care. While the reproductive healthcare providers we spoke with worry about patients' access to abortions, particularly when they are from out-of-state or are going out-of-state, providers' most acute concerns center on the possibility that those patients could present with complications which require medical intervention *after* returning to their home state. While the reproductive healthcare providers we spoke with are sensitive to the need to manage EHR data flow, most do not view EHRs or patient devices as vectors for abortion-related prosecutorial threats and certainly do not provide counseling to patients on device privacy.

Ultimately, we find that, among the reproductive healthcare providers we spoke with, threat modeling around HIPAA is premised on a slightly limited or outdated view of patient privacy, where the primary threats to patients are disapproving or abusive parents and partners, or immigration authorities. In the post-Roe era, there appear to be gaping holes in HIPAA protections, as it does not safeguard EHRs from flowing across state lines, nor from authorities who gain access through physical devices (e.g., [112, 124]) or through tech companies and other data brokers (e.g., [35, 45, 107, 131]). Very rarely do the providers we spoke with suggest (and even then, subtly) to patients that medical records related to their abortion could end up in the hands of other providers or the

[4]The panopticon is a concept for a prison design proposed by English philosopher and social theorist Jeremy Bentham and then applied by Michel Foucault as a metaphor to describe the disciplinary power of societal norms. In the panopticon, inmates are observed through a single watch tower. Although it's not clear if they are being watched, the threat ensures their obedience. Foucault's conceptualization has been applied to describe social media [87] and our Internet-connected devices [60] in a society where, even if we are not being paid attention to, the threat of being watched ensures obedience.

state. This is largely because the providers that we spoke with are not necessarily cognizant of the larger digital landscape of the privacy risks patients face. While it is arguable whether it is the provider's job, or even obligation, to provide digital privacy guidance to patients—to cauterize the data leakage from devices and databases not protected by HIPAA—they are nevertheless well-positioned to provide this guidance.

We argue in this paper that, in order for there to be true informed consent for patients receiving care, providers need to take into account the larger digital landscape of privacy risks. There is significant missed opportunity to equip patients with appropriate safeguards to protect themselves from criminal prosecution. We conclude with preliminary recommendations on how reproductive clinics can better inform their patients about these risks and help protect them in mitigating privacy threats.

With this work, we contribute (1) a hypothetical threat model to illustrate the data flows and related prosecutorial threats for someone who gets an abortion, as context for understanding and contrasting with reproductive healthcare providers' thinking about their patients' abortion-related privacy threats, (2) an overview of reproductive healthcare providers' privacy protocols and practices, (3) insight into the tensions and challenges surrounding providers' privacy practices in the context of abortion, and (4) guidance on how to better support reproductive healthcare providers' abortion-related technology privacy literacy and protocols.

2 BACKGROUND AND RELATED LITERATURE

At the time of this writing, 24 states in the U.S. impose harsh restrictions or outright bans on abortion: 10 ban it at various points from 6 weeks (2 states) to 18 weeks, and 14 impose a total ban on abortion after conception, in some cases with civil and criminal penalties and with exceptions for the life of the mother [5]. Many of those states have signaled an intention to enforce bans aggressively, and while strict enforcement can undoubtedly have a chilling effect, it's also not exactly clear what that means for healthcare providers in legal states. Healthcare providers who perform abortions currently bear the brunt of criminal repercussions. Patients' abortion records and surveillance of their movements and digital behaviors may be used to prosecute physicians or others involved in their care (e.g., parents, partners). In the years leading up to Dobbs, the U.S. has a seen a dramatic rise in use of "fetal harm" laws that allow for prosecution of people capable of pregnancy for their behavior while pregnant [18, 64, 71, 83]. At the time of this writing, a quarter of all states in the U.S. present severe risks of criminal penalty for obtaining abortion [47].

Reproductive health providers have historically been acutely aware of privacy threats. Most consider their duty of care and professional responsibility to include safeguarding patients' privacy against various incursions, whether from family members, intimate partners, or broader community members, including employers or others in positions of power who may object to patients' choices [48]. In this section, we discuss these traditional sources of threat and how digital technology has complicated them. Our review focuses primarily on HIPAA, as it is the only explicit legal protection for patient health data, though it has critical limitations that we highlight based on the available literature. Given our heavy reliance on case studies, we reference numerous news articles and books that cite public documents (e.g., [64, 67]).

2.1 EHRs and the 'commerce' of interstate data[5]

It has become clear that despite presumptions about the protections HIPAA affords, these protections are limited in the face of enforcement of state law. HIPAA does not serve as a legal barrier to the seizure of records through patients' devices, and healthcare providers can be made to hand over HIPAA protected records with a warrant [28, 59, 106], and even without one [129]. While states that permit abortion may preserve the privacy of health records, it remains possible for those records to be seized [4, 75, 78] or to follow patients back to states where abortion may be illegal, where they can be accessed by other providers [143].

[5]Statements in this section were subject to legal review.

Healthcare law experts argue that, in states where abortion is illegal, HIPAA is not a barrier to subpoenas or warrants, and physicians must theoretically turn over records when compelled [137, 143]. Thus, in environments where reproductive healthcare has been criminalized, EHRs that cross state lines may become evidence of criminal behavior.

Zubrzycki refers to the fluid exchange (and changing legal status) of records as the "abortion interoperability trap" [143]. They argue that even states protecting providers from disclosing medical records in out-of-state abortion investigations do not consider that medical records often cross state lines, compounded by recent shifts in federal regulations promoting a "seamless flow of medical records." Scholars warn that this presents particular risks for individuals who travel out of state for abortions and later experience complications upon returning home [41]. They suggest that pregnancy and abortion care are "viewable across institutions within one's EHR, regardless of where that care was provided and whether it was illegal in any of the states where it can be viewed" [74]. Even if a patient presents with a miscarriage, their EHR might convey a different narrative regarding their "decision and efforts to pursue abortion elsewhere" [41]. The sharing of EHRs with other covered entities, such as healthcare providers in different practices and states, is generally deemed essential for continuity of care, reducing redundancy, and ensuring safety [34].

Several states have implemented (or are considering) laws to protect medical records. Connecticut is an example of a state with a shield law that restricts release of medical records to plaintiffs to satisfy "bounty" laws [22, 50], such as those in Texas [29] and Idaho [91] that allow citizens or family and extended family to sue anyone who "aids and abets" [29] or performs abortions. The District of Columbia [3], Minnesota [101], New York [132], Maryland [6], and California [26] have all pursued some type of shield law that limits access to health records by out-of-state law enforcement. The California law goes a step further, preventing law enforcement from "cooperating with out-of-state prosecutions related to abortion, contraception, or gender affirming care" and prevents technology and social media companies from disclosing to law enforcement "any private communication of patients regarding health care that is legally protected in the state" [26]. But as Zubrzycki points out, these laws do not provide protection once records leave the custody of an in-state healthcare provider [143], and laws passed or proposed targeting reverse keyword warrants [126] and geofencing [25, 58] still don't address the issue of medical records.[6]

To illustrate the stakes involved, Zubrzycki describes a hypothetical scenario in which a patient from Louisiana—where abortion is illegal—travels for an abortion to Connecticut—where abortion is legal and there are shield laws. That patient's abortion medical records could be shared with their home-state practice without violating privacy laws. This scenario not only places the patient at risk of prosecution but also exposes the home-state physician receiving the records to potential legal repercussions for failing to report the patient or for withholding the records [143]. Furthermore, it remains uncertain whether federal law prevents physicians from sharing abortion records in a patient's home state, even with new changes to HIPAA [8, 109]. Turning off that sharing of EHRs across providers might be a solution, but as Zubrzycki points out, federal laws are increasingly imposing sharing of those records. [7]

Shield laws protect physicians from being prosecuted for performing abortion for patients from illegal states, but it's becoming increasingly uncertain how these protections will hold up in practice [22] when laws like the one recently passed in Idaho against against so-called "abortion trafficking" make it a crime to help a minor get an out-of-state abortion without parental consent. As written, this law reaches across state borders to raise the prospect of prosecuting physicians who provide abortions in a state where abortion is legal [38]. The HHS Office

[6]The My Health My Data Act does protect health data that falls outside of HIPAA regulations (e.g., restricting sale of consumer data that could be triangulated to reveal or predict health status or outcomes) but it still doesn't protect medical records or other data generated by individuals related from warrants or that travel out-of-state.

[7]Zubrzycki puts a fine point on it saying that "prosecutors or litigants could circumvent Connecticut's safe-haven protection by subpoenaing any other provider with access to her abortion records" [143].

for Civil Rights (OCR)—which enforces the privacy rule under HIPAA—did offer clarification that reporting is not permitted for abortions, even in states where abortions are illegal, *but only if* there is no specific legislation mandating they be reported [106]. That said, EHRs could still be obtained through a court order by authorities in any state [109], and changes in state laws might create additional grounds for reporting. Despite impressions that HIPAA provides stringent protection of personal health information, it does not necessarily withstand enforcement efforts by state agencies seeking to prosecute violation of abortion laws, particularly since there are alternative ways of securing information.

Law enforcement can request medical records from healthcare organizations based on "tips" from friends, family, partners, and others [84, 115]. They may also make blanket requests of records from reproductive clinics or funds [4, 116], and healthcare providers may be forced to comply [75, 78].

Finally, law enforcement can also make requests to providers' business associates [41]. Insurance companies, too, have access to patient health records, and with the introduction of ICD-10 codes for greater billing accuracy, it may be more difficult to conceal abortions. Clayton et al. provides scenarios that illustrate some ways privacy incursions can occur by those willingly handing over EHRs [41]. For example, a healthcare organization employee could obtain access to PHI, or could search for "complications of possible abortion," regardless of where it occurred [41] and alert law enforcement—even if these data are protected, there are many cases where healthcare providers have reported patients [62, 64, 71].

2.2 Third-party data and devices—the threat model beyond EHR

It has become clear that the protective circle established by HIPAA is highly penetrable. However, there are equally, if not more, serious concerns regarding the risks to privacy associated with information that HIPAA was never explicitly intended to safeguard. For instance, third-party apps and devices are not bound by HIPAA regulations. Data from healthcare portal downloads, non-HIPAA apps, search histories, social media, messaging, geolocation, and more may be accessed through warrants—served either to the patient's own device or to third parties—including blanket geofencing and keyword warrants. Law enforcement may also obtain this data through direct purchases. Below, we characterize the risks associated with three types of data: information that appears to be protected by HIPAA, health-related data that is not protected, and personal data that lacks protection altogether.

2.2.1 Seemingly HIPAA protected data. While data from healthcare portal apps may be considered protected by HIPAA to some extent, companies providing these services often sell patient data and may claim they are not subject to these regulations (e.g., [53]). Since the onset of the COVID-19 pandemic, there has been an influx of health apps that circumvent HIPAA protections [44]. Hospitals frequently sell deidentified patient data to third parties, including technology and pharmaceutical companies, market researchers, and consultants [137]. Although the data within the portal apps may theoretically be protected by HIPAA, it may be that they rely on third-party servicesthat are not fully compliant with these regulations.

Moreover, according to HHS, healthcare providers do not always use HIPAA compliant services, or know whether data are available to third parties [107]. Research has shown that deidentified data are not as anonymous as we might think [82]. Anti-abortion organizations have reportedly tracked individual visits to hundreds of abortion clinics across the U.S. using location data from data brokers [65, 96]. It is also possible to gain access to identifying information of individuals who schedule abortions on clinic websites through third parties like Google, Meta, and Tiktok [68]. The OCR recently issued a bulletin clarifying that, in cases like these, third parties act as business associates ("regulated entities") that are subject to privacy rules [108]. While this could stop purchase of these data by law enforcement and hostile organizations (though it seems to have not), it doesn't necessarily stop subpoenas or warrants for this data.

Furthermore, when patients download any health-related information from health portals to their devices, that information is not protected. According to HHS, "HIPAA Rules generally do not protect the privacy or security of your health information when it is accessed through or stored on your personal cell phones or tablets" [107]. This means that electronic health records (EHRs) transferred to patients' devices are not protected [41]. Patients may also link their health records to third-party applications [105] (for instance, Epic EHR software can connect to a Fitbit [7]) or use other unprotected apps associated with their reproductive health activities.

We do not know what individuals know about the privacy implications of their health apps and/or mistakenly believe that HIPAA applies to their health data, including data on their phones. It is certainly understandable for people to expect that health records would be safeguarded on personal devices.

2.2.2 Seemingly private but not HIPAA protected data. Patients can reveal aspects of their health records pertaining to abortion in more oblique ways, simply through everyday engagement with browsers, apps, or geolocation data.

The vast majority of health apps, including period trackers, share health and other data with third parties [9, 11, 90, 117], and these apps remain largely unregulated. This issue is fairly well known, particularly regarding the threats posed by period trackers [85]. Notably, law enforcement has purchased period tracking data to monitor pregnancies among immigrants in the U.S. [43, 139]. Geofence [10] and keyword warrants [43, 127] may also enable authorities to request information on individuals who have visited abortion clinics across the U.S. or searched for information about gender-affirming care [126]. Moreover, authorities may be able to purchase this data directly (e.g., [45, 126]). Additionally, some online providers of abortion pills utilize trackers whose data is accessible to Google and may easily be intercepted or purchased [63, 72].

Data brokers allow law enforcement to do an "end run" around [35] legal restrictions, simply buying data that would otherwise require a warrant [45]. This workaround might grant access to various types of data, including internet searches, purchases [79], geolocation data, even license plate data [36, 37].

2.2.3 Personal device data. Law enforcement can also use data from search histories, online purchases, and messaging on individuals' devices in investigations about abortions [112]. In her review of investigations of abortion crime in the U.S. and the role that digital media plays in giving law enforcement access [43], Conti-Cook asks us to:

> "Imagine what Jane—the underground abortion network that grew out of Chicago in the pre-Roe late sixties—would look like today if abortions were criminalized. Instead of hanging flyers on campuses and putting advertisements in newspapers that read 'Pregnant? Don't want to be? Call Jane,' in today's world, there may be Instagram accounts, websites, email addresses, and a Facebook group where members connect instead of meeting in person." [43]

The phone in our pocket loaded with GPS and search apps, partners and family with whom information is shared freely or inadvertently, and even protesters in parking lots with cameras—all these and other forms of exposure—present risks. Advocacy organizations that publish guidance on reproductive health and cybersafety, such as the Electronic Frontier Foundation (EFF), warn that one of the greatest threats to patient privacy is device searches that result when healthcare providers, friends, or family report individuals they suspect of having had an abortion to law enforcement [57].

In several instances, law enforcement has utilized text data in the criminal prosecution of people capable of pregnancy suspected of having had abortions beyond what is permitted by law [70, 75, 112]. Recently, social media and messaging apps have also been employed in abortion-related prosecutions [70, 84]. For example, in the case of a Nebraska woman charged with helping her daughter obtain an illegal abortion, Facebook complied with a subpoena and provided data to authorities [70]. In Mississippi, online searches for abortion pills were used to charge a Black mother who miscarried with killing her child [124, 141]. Precedents for such digital searches

can be traced back to 2015, when Indiana sentenced a woman to 20 years for feticide and neglect based on text messages exchanged with a friend discussing her abortion and digital receipts for abortion pills, mifepristone and misoprostol. Her sentence was later reduced on appeal [112].

Prior work suggests that concerns about social media as it relates to abortion are focused on what people say publicly, but not what is shared on private messages [85], even though they can present risks. Police can also monitor social media without warrants or direct access to devices because, for instance, social media platforms give access to keyword searches in posts "geotagged within their jurisdiction" [43].

2.3 Patient medical data and provider communications in HCI and CSCW

Human-Computer Interactions (HCI) and Computer-Supported Cooperative Work (CSCW) literature has looked at the disclosure practices of individuals seeking health related support on social media [12–15, 135]. Some studies have looked at the disclosure expectations and practices of patients, noting misalignment when patients share data that they had not expected would be shared [40]. In presenting the concept of contextual integrity, Nissenbaum talks about how context governs the flows of data, using an example of patients and doctors [97]. She argues that while it's obviously appropriate for a doctor to inquire about a patient's sexual health, the same is not true for the patient—it's not appropriate for patients to inquire about their doctor's sex life. Others have applied these contextual phenomena to understand the norms of information flow that govern healthcare interactions [100]. However, one issue with traditional privacy theories, such as contextual integrity, is that they do not account for the fact that patients and healthcare providers may not be fully aware of where and with whom patient data is shared, highlighting the infinite extensibility of risk inherent in digital technology.

2.3.1 Informed consent. Medical informed consent is key to providing care and treatment in healthcare, in part because it is perceived to promote trust [51]. The concept of medical informed consent dates back to the post-World War II Nuremburg Code, designed to prevent unethical research [118]. It involves disclosures that allow individuals to understand the risks and benefits so that they can make "informed" decisions. The requirement of informed consent is also used in the digital privacy space to describe generally the process of informing individuals about how their data is being collected, used, and shared, and for what purposes. While the laws governing informed consent by tech companies vary by region and state—with some having more stringent requirements for disclosure, like California as part of the California Consumer Privacy Act (CCPA)—it is nevertheless nearly impossible to read through user agreements on devices we use [103, 142].

While in the medical context, the concept of informed consent has historically referred to patients' knowledge about a procedure [23], it is increasingly used to describe patient consent to sharing their health data. Literature looking at informed consent in the healthcare context has found that patients do welcome access to personal health records to manage conditions and communicate with their healthcare providers [66] and can play an active role deciding how and with whom their data is shared [61]. But it's also not clear how this plays out in the complex and ever-changing terrain of reproductive health, particularly if there is a perception that HIPAA offers more protection than it in fact does [19, 21, 51].

2.4 Vulnerable populations and their privacy needs

HCI, CSCW, and related fields are increasingly investigating ways to study, frame, and support privacy for vulnerable populations [86, 88]. We define vulnerable individuals as those particularly "at risk" of privacy violations [134] because of their race, socio-economic class, gender, sexuality, other identity facets or circumstances that marginalize them from society, and intersections thereof [88]. Vulnerability is particularly evident in sex work and harassment [120], reproductive rights, and parenting [33, 49, 64].

Vulnerable individuals are often stigmatized by the law, and when it comes to their rights, are often considered second-class citizens. For example, survivors of sexual abuse are historically subject to "digital strip searches" to

provide evidence for their rape, a practice that in the UK ended in 2022 [2]. Legal scholar Khiara Bridges uncovers the racist, stereotyped privacy incursions that poor pregnant women of color face when they seek support in the U.S. social welfare system [33]. Similarly, Michele Goodwin points to how the U.S. criminal justice system attacks poor pregnant women of color, including prosecution for miscarriages [64]. Both Bridges and Goodwin suggest that being pregnant, particularly for low-income women of color, strips away fundamental privacy rights guaranteed to more privileged individuals.

In Alabama, for instance, "chemical endangerment" laws are used to arrest and imprison people capable of pregnancy suspected of using illicit drugs while pregnant until they receive treatment, or are released by a judge [69]. In Oklahoma, a woman who used medical marijuana prescribed by her doctor was charged with "felony child neglect" in 2021; since then, Oklahoma has seen a number of similar cases [17, 62]. In California, a woman was jailed for a stillbirth when found to test positive for drugs [77]. More recent efforts test interstate laws around minors seeking abortions [38, 115] and gender-affirming care [75, 78]. These cases, along with others involving IVF, [140] are setting the ground for constitutional battles that will likely widen the space of vulnerability.

In this post-Roe era, we include in this category of "vulnerability" individuals susceptible to prosecutorial threats because of the fact that *they can become pregnant*. This vulnerability is compounded by various factors, including the laws of a given state, as well as age, race, sexual orientation, and reproductive (and related health) risk [85]. Like Collins, we understand vulnerability as shaped by laws, cultural norms, and structural inequalities [42] alongside other contextual factors. This perspective is critical because research suggests that individuals with insight into the nuanced struggles of vulnerable populations are better equipped to provide tailored, intersectional privacy guidance [80, 89, 119].

Post-Roe, an exponentially broader population is at risk, a fact that may be overlooked as reproductive healthcare providers concentrate on their traditionally vulnerable patients—those individuals whose primary threat are partners and family members. While these vulnerable patients offer valuable insights into how providers manage privacy incursions, this focus may also leave providers unprepared for a landscape where threat vectors now include law enforcement, in addition to abusive or disapproving family members.

2.5 Healthcare providers and security guidance for vulnerable individuals

In the HCI and related security literature, some evidence suggests that providers are well-equipped to offer privacy and security stewardship to vulnerable populations, especially when facing a combination of complex threats (e.g., law enforcement, disapproving or abusive family) [80, 89, 119]. The significance of privacy data stewardship has also been highlighted in the context of intimate partner violence (IPV) [125].

However, there are circumstances in which healthcare and other providers struggle to offer guidance. IPV is particularly instructive in this regard, as the threat vectors involved are so intimately intrusive. In a study involving IPV survivors and professionals—such as case managers, social workers, attorneys, and police officers— Freed et al. found that both groups often lack the expertise to identify or mitigate technology abuse, including access to social media accounts [55]. IPV professionals expressed frustration over their inability to keep up with rapidly evolving technology, often resorting to "google-as-they-go." Despite this, some professionals have discovered online resources and guides that provide useful "high-level" advice for ensuring digital safety [55].

Freed et al. also identified several challenges related to the guidance healthcare providers offer, including a lack of actionable advice, absence of best practices, and extreme recommendations that may seem unfeasible (like disconnecting all devices). In another study focused on IPV, Freed et al. found that the intimacy of our devices and the availability of ready-made surveillance applications render threats exceedingly difficult to circumvent [54]. Recent work by Tseng et al. underscores the challenges of designing infrastructure that can provide technical consultations to IPV survivors [125].

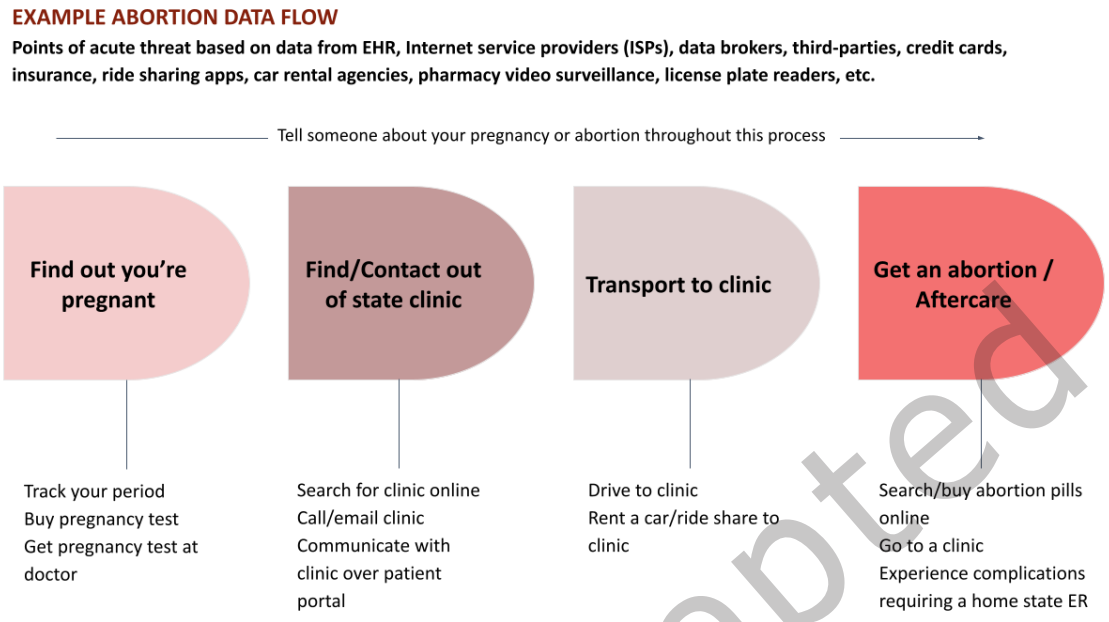

Fig. 1. Potential data flow of a hypothetical "Jane" from the time they suspect they are pregnant to after getting an abortion.

There are certainly parallels with recent abortion prosecution cases in terms of the inability to keep up with the digital vectors of threat. Experts note that there are "many, many data points we might not even know about that law enforcement authorities might be able to subpoena and use" [81]. Yet from case law that we have gathered, we can at least start to depict scenarios that, while complex, map relationships between sources of threat across various complex vectors of threat,different contexts, and data and non-data surfaces.

2.6 Threat modeling the reproductive healthcare space

Threat modeling is a method used by technology developers to play out security vulnerabilities and develop countermeasures during the process of development [123]. It involves "identifying assets and attack vectors as well as archetypical attackers, their motivations, goals, and knowledge of the system/organization" [52, 93]. As a formal process, threat modeling has its origins in Microsoft, which introduced the STRIDE security threat model, developed for Windows [76]. In 2004, Swiderski and Snyder wrote the seminal text "Threat Modeling," in which they further developed the concept [122]. User studies of threat modeling have largely focused on security practitioners (e.g., [56, 121]) and it is not clear how this method might be developed and used by people without technical backgrounds.

As laws change and we learn more about what data is available to authorities, it has become clear that, in the abortion context, threat modeling encompasses vast ecosystems of data available and vulnerable to seizure through numerous mechanisms. In Figure 1, we show an example of many data points that could be gathered if someone were receiving a hypothetical out-of-state abortion. One challenge with constructing these data flows is that, at any point, data could be given to multiple service providers and third parties, and healthcare providers who themselves may be subpoenaed. For example, HIPAA clearly does not protect patients who show up in the

emergency room and are reported for suspicious miscarriages [43, 104, 112]. Moreover, any one of these examples of digital evidence we have so far described can be obtained once police have access to someone's devices. Service providers can (and have) circumvented privacy rules when they feel that a crime has been committed [59].

Based on our research and discussions with legal experts, we developed the abortion data flow (Figure 1) and accompanying scenarios (Table 1, see Appendix) to show the acute threats that someone *could* face during their abortion journey. **Figure 1**: shows this simple data flow from the point at which someone suspects they are pregnant to after they receive an abortion. These threats are complex and dynamic because the digital and legal threats are being tested and litigated. As such, this figure is merely illustrative and does not represent the extent of all possible threats. **Table 1 (see Appendix)**: elaborates on examples of the data flows and accompanying scenarios that went into the creation of this diagram.[8] In table 1, we also further label these flows and scenarios in three categories defined by the "status of threat": "data flows exist" to suggest that obtaining data is possible, "experts have expressed concerns" to convey that lawyers, advocacy organizations, etc. are wary of data being used in criminal investigations and prosecution, and "case law exists" when these scenarios have actually happened (for example, the Nebraska case [70]). We included example sources for these data flow scenarios, but there are many articles which we read but did not list. This threat model diagram and table are useful to contextualize how the reproductive healthcare providers we spoke with are not equipped to fully take into account the risks that patients face at every stage.

To our knowledge, there is no research on the ways that reproductive healthcare providers are threat modeling privacy for their reproductive health patients and the challenges they face in doing so.

3 METHODS

3.1 Participants and interview protocol

We recruited participants during fall 2023 from a health organization that provides reproductive-related services, including abortions. They disseminated a flyer about the study to clinics across the U.S. Because this was a highly sensitive topic, we specified in our flyer only that we were looking to talk with people who treat vulnerable patients about the privacy guidance they offer. We did not want to advertise that we were recruiting about reproductive health (and more specifically, about abortion) for fear of drawing attention from bad actors or putting our participants in legal jeopardy. But we did ask that the organization communicate this informally alongside our flyer. Participants that came to the interviews thus knew what our research was about.

Participants were directed to a screening survey where they were asked if they worked in a reproductive care setting or provided those services in an adjacent setting. They also answered questions about their role, practice, state, and the demographics of their clinic and themselves. We contacted a subset of those who took our screener and provided an email address. They were given the option to use an encrypted email for the purposes of communicating with us about this study. We focused on inviting diverse participants from various states, roles, and practices. In all, 89 individuals completed the screener and provided an email contact. We sent out 46 invitations. 22 participants completed the interviews. We spoke with people who reported being: an assistant who provides counseling services to patients in a reproductive care practice or setting; advanced practice clinicians (APCs), including physician assistants (PAs), advanced practice registered nurses (APRNs) and certified nurse midwives (CNMs) in a reproductive healthcare practice or setting; OB/GYNs providing reproductive care; social workers or healthcare-adjacent roles providing reproductive health advice or guidance; and medical professionals providing reproductive health advice or guidance. We refer to the individuals we interviewed as "providers"

[8]For the sake of space and comprehensibility, this table does not elaborate on every iteration of the threat, nor does it provide data type and data holder information. Threat modeling is highly contextual and somewhat idiosyncratic task and so we provide this diagram and table as an illustration of the types of threat modeling one could do.

throughout our findings. We ultimately spoke with providers in 7 states across the U.S., including 4 in states that are protective of abortion, 2 in states where abortion is banned, and 1 in a state that has restrictions on abortion.

Although, as earlier noted, we relied on word-of-mouth to inform participants about the subject of our interview, we also told participants before recording that we were interested in their abortion-seeking patients and asked if they felt comfortable continuing. We provided them with ample detail about our privacy procedures but also advised them to obscure their organization, location, and other details that may have been revealing on the recording. After describing our interview goals, we told participants that they could opt out or stop the interview at any time. We also told them that we could redact anything that they were uncomfortable with.

We used a semi-structured interview guide that asked about privacy protocols used in the clinic and unmet privacy guidance needs. While participants were told up front that we were particularly interested in talking about their patients seeking abortion, we invited them to define who they worry most about being vulnerable to privacy related harms. Interviews lasted an average of 40 minutes. Participants received a $95 gift card as an honorarium.

3.2 Privacy and ethical considerations

We took a number of steps to protect our participants: We did not link the participant data we stored with any identifying information, such as name or email. We used an encrypted email to set up interviews, did not provide calendar invites, and deleted exchanges after interviews were complete. We used a burner phone to contact participants and did not leave voicemail if they did not pick up. We did not share honorarium information over encrypted email, but provided it over the phone at the end of the interview; participants were told if they misplaced it to email us requesting that we call them. We recorded interviews on a non-internet-connected device. Interviews were transcribed by an open-source transcription tool running locally and manually redacted. We do not report on participants' demographic details. We have removed all identifiers from quotes.

Interviews were conducted by one of two researchers, but because of our privacy protocols, each interview typically had one or two additional researchers listening to the interview and taking notes that were stored on our secure file store. Note-takers listened over FaceTime audio, which we deemed to be secure, for listening to the interviews being conducted on the burner phone. Our study was approved by our IRB.

3.3 Analysis

Our approach to analysis is informed by critical phenomenology [136] and reflexive thematic analysis (RTA) [30, 31]. Phenomenology generally seeks to "bracket" [114] the perspectives of the researchers and allow participants' beliefs and context to shape understanding of a phenomenon. Our framing, however, is informed by surrounding structural, ethical, and political considerations that influenced our presentation of findings. For this reason, we sometimes point out in our findings where interpretation of laws or technology were not correct. We did this cautiously, while also demonstrating how these perceptions produce meanings in the data.

RTA allows us to identify patterns in the data and construct a narrative. These "compelling interpretations" involve the researchers' experiences and the expertise [32] that the researchers bring to bear on this analysis. In practice, RTA involves familiarizing oneself with the data, open coding, generating initial themes, reviewing those themes, defining and naming those themes, and writing up the results. The three researchers who conducted the interviews spent 10-30 minutes debriefing after each call to (early on) make adjustments to the protocol and (throughout) identify and discuss codes and themes as well as additional probes and questions to prioritize.

At the conclusion of our interviews, three researchers went through the transcripts to identify codes and themes used to organize our findings. We went through further iteration to review and refine the names of those themes. Data were transcribed and stored on a secure data repository where we could not take notes, so the themes and quotes were written down on paper with associated participant codes. While these interviews

were focused on abortion related privacy, providers discussed other vulnerable groups as noted in the findings. We identified themes around different protocols that related to different threats (the physical clinic, EHR, and communications within and outside their walls). We also identified additional themes around abortion scenarios where providers expressed concern that they could not provide privacy and/or where we noted the shortcomings of their strategy—where we do, as mentioned, break from our phenomenological approach. This work was reviewed by lawyers to ensure that participants (e.g., who talk about breaking the law) are not at risk.

3.3.1 Researcher background and positionality. The researchers involved in this study have backgrounds in reproductive health and technology research, medical provider research, and privacy and security.The team's approach to this research was further informed by extensive research on the digital and legal risks associated with abortion in the U.S., starting as far back as the last century to the present day.

3.4 Limitations and reflections

Although our sample was diverse in some ways, more diverse perspectives and contexts could have been represented (as is almost always the case in interview studies). We worked hard to ensure the diversity of participants both geographically and demographically. While we attempted to reach other organizations, we were unable to, which may have limited the diversity of perspectives. We attribute this limitation to the sensitive nature of the topic. In order to preserve privacy and ensure the comfort of our participants, we refrained from asking (or reporting) too many details about practice location, size, organization structure, etc. To protect our participants, we do not elaborate further on ways in which our sample was (not) diverse and how this might limit generalizability. While our findings, like most interview studies, are unlikely to generalize to all providers and clinical contexts, we identify important gaps in privacy understanding and knowledge, and we argue that addressing these gaps could provide broad benefit.

Given the sensitive nature of this topic, it is possible that participants may have been wary of speaking with us. We spent significant time at the beginning of our interview explaining our procedures, including the use of non-internet connected devices. We told participants they could redact anything they ultimately felt uncomfortable with and we did also warn them when a topic might bring up illegal activity, such as providing or facilitating abortions. Participants acknowledged that they understood the risks, and some did obscure their organization and location while speaking to us on record. Based on these interactions, we felt that we received thoughtful responses. Please note that any direct reference to illegal activity has been obscured or removed to protect the safety of participants.

4 FINDINGS

In our findings, we detail privacy controls currently in place within providers' clinics, highlighting how providers think about abortion-seeking patients' privacy relative to their other vulnerable patients. We then address tensions and challenges surrounding abortion and how providers conceive of associated privacy threats, particularly as it relates to whether abortion is legal or illegal in their state. Below we first overview and situate our findings.

4.1 Overview

Providers consider minors, patients seeking gender-affirming care, those with disapproving or abusive partners, and those seeking abortions among their most vulnerable in terms of privacy encroachment. However, abortion-seeking patients are not necessarily top-of-mind on this list. In our interviews, we found that providers are most conditioned to think about privacy and vulnerability in contexts that are not primarily about abortion, in part because many threats related to abortion are relatively new. Accordingly, providers are conditioned to prioritize adversarial risks and privacy violations emanating from families and partners over those from authorities and state actors. For this reason, we include providers' perspectives about caring for other vulnerable

patients, abortion-related or not, as context and contrast with providers' abortion-specific privacy practices and perceptions of threats. We report on what providers told us the protocols were in their practice and their perceptions of the reasoning behind it. We are not representing "clinics" in these interviews as we did not talk to multiple individuals from the same practice or from certain clinic "types" in any consistent way.

While we observed some variation in reported privacy protocols and practices related to physical privacy and communications, EHR flows, and subpoenas for records by law enforcement, we did not see any trends based on clinic setting (urban or rural). Furthermore, we make no claims of prevalence for any specific privacy and security technique; rather, we seek to provide an overview of how providers think about and address privacy threats. Notably, we cannot verify that these protocols and practices reflect the policies of the clinics where they work, only what providers told us.

Providers in states where abortion is legal are concerned primarily about keeping patients' information confidential within the physical space in which they care for patients (including from other office employees and people who accompany patients). These providers are focused on carefully managing EHR information flows, worrying about exposure to family or partners, rather than other providers. This focus has historically been on patients seeking legal care, and providers often perceive HIPAA as protecting their patients from threats, without fully taking into account that other providers with access might themselves be threat vectors.

Patients seeking legal abortions are also a concern, insofar as these decisions can be contentious even when not illegal, but abortion care and counseling remains set apart by habits of thinking and limited experience with emerging challenges. Providers do express specific concern for patients seeking abortions from out-of-state, but the thrust of this concern is medical in nature. The concern for out-of-state patients is centered around their abortion aftercare needs when they return to their home state, as opposed to consideration of the digital data that could incriminate them.

For providers practicing in states where abortion is no longer legal, the focus is on getting patients the information needed to obtain an abortion in a safe state (although providers cannot always refer or make appointments directly) and offering funding and logistical support for those efforts. While mindful that patients have a set of distinct challenges arising from this new landscape, providers mostly do not express concerns about patients' personal devices and other digital privacy and, when asked, assume that this is being dealt with by others, such as advocacy groups, that help connect patients with referrers and providers in legal states. A few providers are careful to represent a patient as merely considering an abortion, rather than committed to obtaining one. This ambiguity presumably gives patients both privacy and space to deliberate, thus supporting patient autonomy in decision-making while simultaneously affording some protection against legal repercussions.

Providers in both groups do not worry much about broader EHR threats beyond family or partners, or about subpoenas or warrants, nor do they give patients advice about digital data or devices. With attention squarely on their own environment and locus of control, providers are not equipped to entertain hypothetical threats. Providers are accustomed to considering EHRs as fully protected by HIPAA and have not yet considered or become aware of alternative scenarios. Doing so would require a kind of thought experimentation and perspective well beyond their current focus and range of experience.

Our findings reveal that providers rarely engage in proactive threat modeling for their clinics, aside from the minimal measures mandated for HIPAA compliance. HIPAA compliance requires that they not disclose information about a patient to an unauthorized entity (such as a parent or school) but it does not prevent EHRs from being shared with other covered entities, such as healthcare providers in other states. We nevertheless apply the abstract threat model introduced in this paper to our analysis because few consider the presence of state adversaries who leverage the gaps in HIPAA protections, or other legislative and prosecutorial techniques—techniques that providers themselves do not think about or are unaware of.

4.2 Current privacy controls in place

We outline privacy protocols and practices that address potential threats both within clinic settings and in the broader context, such as during electronic health record (EHR) sharing with other practices or insurers, or in the event that these EHRs are subpoenaed.

4.2.1 Privacy and security in the clinic physical space. All participants work in clinics where privacy protocols govern communications with patients occurring within the clinic setting. Providers prioritize establishing zones of physical privacy for their patients. This includes limiting device use, carefully controlling who accompanies patients, selecting and vetting translators, and monitoring the accuracy of translations for patients who are not comfortable speaking English. Many clinics prohibit cell phone use in waiting and treatment areas, and providers are careful when discussing patients to avoid using names or being overheard discussing them.

> "No FaceTiming. No calls during the actual visit. We do have signs in the lobby, no phones either."

Providers ask patients about, and also closely monitor, family and partners who escort patients to see whether patients are uncomfortable with their presence.

> "Because of the services that we provide, we get couples that aren't on the same page. So we have the patient come into the room first, and then we ask the patient if they want someone in the room for the ultrasound instead of automatically allowing both those people to come in because we've had cases where they're like, 'No, I don't want them in the room.'"

Providers take patients to the exam room alone, not only to establish that the patient feels safe with the person accompanying them being in the room, but also to address sensitive questions and get candid answers.

> "So if a patient has someone with them, when they come to the back to be put into an exam room, we bring the patient back first. We go through all of their risk assessment questions and all of that … We're talking about like, 'Are you safe in your relationship? Is everything consensual? Are you in a safe living environment?' And then talking about what's going on, number of sexual partners, all of that. We do that privately before anyone else comes back."

Practices extend these strategies to patients who are not comfortable speaking English by monitoring translators to discern whether they are personally acquainted with patients. If so, the clinic may offer an alternative translator. Providers are also vigilant in ensuring that patients are not misled about the procedures being performed—for example, believing they are receiving a COVID booster instead of STD medication.

4.2.2 Communication privacy beyond the clinic. Communication privacy extends beyond the walls of the clinic. Providers ask all patients screening questions to determine their preferred methods of communication after they leave the clinic. A critical objective is to ensure that patients can receive and transmit information securely, without the risk of interception by household members or employers, which would constitute a violation of HIPAA.

Providers are adamant about knowing who they can safely share information with and by what means, since they worry about negative consequences or abuse from family or partners if patient information is disclosed. In this regard, providers are particularly concerned about minors seeking birth control or STD testing, patients seeking gender-affirming care who have disapproving family, and patients with abusive partners.

> "Interpersonal issues, which can be anywhere from inadvertent disclosure of information the patient wouldn't have wanted to share that could be embarrassing all the way up to threats of death … an unfortunately not uncommon scenario is having a patient whose partner accuses them of cheating and reports not having any other partners, but the patient now has chlamydia."

Communications screening, typically conducted at appointment check-in, generally includes whether the clinic has permission to leave a phone message or send physical mail, whether providers should send mail without

labels, and whether to address patients by their legal or chosen name in physical mail. Passcodes might be used to ensure that only patients and those they have shared the passcode with can access their records over the phone. Providers indicate that they do not send email for appointments or results.

> "We always ask privacy settings for people. We in family planning serve a lot of folks in the trans community. And so we know [it's not safe for all folks] to have their chosen name on [their mail], things like that. So, we do screening questions to make sure that the mail they're receiving is safe for them to receive at their home."

> "So, one effort to protect ourselves and our patients, information security-wise, is we generally do not use email communication with our patients."

Providers do not necessarily see typical abortion patients as unusually vulnerable in this sense.

> "There are basic things that we talk to patients about … so like the mail questions, the email questions, those are all things that we ask all patients. And then the consent forms for electronic communication and then privacy non-discrimination are the same across all departments. But it's not specific to their abortion information."

In effect, notions of privacy protection—whether digital or interpersonal—are focused almost exclusively on the flow (or leakage) of information between patients and people in their immediate environment. This is a context that providers can conceive of concretely and are often equipped to assess directly based on their own observations and interactions with patients. These descriptions of policies and protocols indicate that providers are vigilant and painstaking about ensuring privacy in the immediate physical environment.

4.2.3 Limiting the flow of EHR data. Almost every provider reports that their clinic uses an EHR system capable of sharing patient data with other providers who also use that system. Providers' concerns about the flow of EHR data vary, but these concerns do not necessarily take into account what is technically possible, and some providers may understate the risk.

Some of the providers we spoke with are sensitive to the potential transmission of patients' electronic data, and may even take precautions to protect it, or may be operating in clinic settings where precautions are already in place. However, we did not observe any trends in this behavior based on the clinic type or location. Some clinics limit what EHR data is shared with other providers by default. Where relevant, we note the strategies of one clinic with an older EHR system that did have more control over sharing; they also noted that sharing as the default is on the horizon.

In other cases, providers ask patients—sometimes all patients, and sometimes specifically those who volunteer privacy concerns—whether they want to limit EHR sharing, or turn it off altogether. Initial screening at the front desk—which, as described above, includes questions about communications preferences and privacy—is used to identify any specific privacy concerns the patients may have. Front desk staff then pass this information to the clinical staff to alert them that further discussion is needed.

> "And if they have privacy concerns, we'll usually also get a message from the front that says opt out, which means opt out of [system that shares records]. So we can just kind of put it in. And then when I get that notification, I'm like, I am opting you out so you can hear me and you know that it's actually happening."

In the infrequent instances when providers do limit EHR sharing according to patient preferences, there are typically two main options: (1) turn off the sharing mechanism that allows for the visit record to be shared with other healthcare providers in their EHR, or (2) restrict information about the nature of the visit. The second option enables some continuity of care across practices, but omits some specifics, such as abortion-related treatment, to prevent those details from being visible to other practices in states where abortion is not legal. Other methods to conceal abortion related care include using aliases and careful word choices. While a few providers suggested that

they can create aliases in EHRs, and have done so, it was not necessarily to prevent other healthcare providers from accessing information, but to make patients feel more comfortable conversing with them about out-of-state arrangements.

A few providers who have the ability to limit EHR flow noted that they explain to patients how EHR sharing works—what information other practices can and cannot see, as well as the rights patients have to opt in or out of sharing.

Among the providers that might default to sharing EHR, some emphasize the importance of informing patients about who can potentially see their records, enabling patients to make fully informed decisions about turning sharing on or off:

> "We're a little more careful, I think, than other offices … A lot of offices sort of default to sharing medical records, and we're a lot more careful about that. Like, we really let patients know, this is what other places can see, this is what they can't. Do you want us to opt you out of that?"

While some providers express concern that patients don't think about EHRs enough, others reassure patients not to worry too much, maintaining that EHR recipient practices don't see "everything"—though it remains unclear to what extent this is true.

> "A lot of patients don't understand that their other providers can't see all of their records all of the time from any visit they've ever had in their life. So, we do a lot of educating on that. And we are pretty stringent about our request of records policies. If somebody's signature is missing or things like that, we won't send any records to any providers without having all of the pieces in place, and if there's any issues you should contact the patient and don't send the records."

Despite this provider's assurance about protecting patients from non-medical individuals seeking access to their records, many EHR platforms facilitate the automatic sharing of records.

Providers varied in their reported sharing protocols as well as in the degree to which they questioned patients about their own sharing decisions. Providers were unanimous in perceiving that their EHR protocols are more stringent compared with medical practices in general. This view of their own relative vigilance would appear to be more presumption than empirical, given the diversity of approaches even within this small sample. Indeed, providers are often constrained in their assessment of what constitutes true vigilance due to limited knowledge and experience. For example, many assume that patient EHRs are not shared across state lines, even though they are uncertain of this. In sum, we did not see any trends in terms of how practices do or do not share EHR data with other practices. Providers with the ability to enable or disable EHR sharing generally consulted all patients regarding their preferences. However, some only did so when patients voiced concerns.

4.2.4 Insurance records. Opting out of sharing EHR with other practices does not prevent diagnostic codes from being transmitted to a patient's insurance company. Several providers mentioned insurance records as a particular concern for minors, who worry about their parents receiving sensitive information via this channel.

> "And I'm like, I am not going to get you in trouble. Who are you worried about getting in trouble with? And they're like, my mom. And I'm like, unless your mom is on your insurance, she shouldn't be able to see this. We can turn off [system that shares patient records] for you … Like minors, especially minors getting abortions, are very concerned about privacy. Unless their mom drove them there."

When discussing confidentiality in medical records as it relates to family and partners, providers often emphasize aligning data-sharing practices with patients' perceived risks. For instance, one provider explained that they assure patients their parents won't have access to their medical records. Another provider highlighted the issue of confidential billing, noting that while it can obscure details like medical codes in explanation of benefits, patients need to actively reach out to their insurance company to ensure this level of confidentiality

4.2.5 EHR and subpoenas. Few healthcare providers recall being subpoenaed for patient records, but those who do often recount incidents from years ago, particularly involving U.S. Immigration and Customs Enforcement (ICE) attempting to access EHRs for immigration enforcement purposes. In those cases, clinics refused to comply with such requests. Providers generally believe that HIPAA offers protection against these types of subpoenas, even though this is not always the case. Their greater concern is that fear of law enforcement could deter patients from seeking necessary care, so they take proactive steps to reassure patients that their records will not be shared with law enforcement.

> "A lot of our patients seem to think that healthcare and government are all intermingled, and we all tell each other everything … we try not to work or tell police anything unless they have to use our cameras because something happened across the street. But a lot of patients who have limited English proficiency or are concerned about their immigration status, they kind of think that like healthcare and government all work together and we all know everything, we all share everything."

Providers take seriously their role in providing comfort and rapport to patients, particularly those who they think are vulnerable because of their identity, age, or immigration status. For these patients, concerns about data leakage can lead to hesitance or refusal to seek care to protect their privacy. In the post-Roe era, however, laws and norms around patient privacy are still in flux, and it remains uncertain whether HIPAA fully empowers providers to resist subpoenas for records related to abortion care [137].

Ultimately, it seems that providers' routine threat models, which focus on local and familiar threats, are not sufficient in a changing landscape where new and different agents are probing for new cracks in the privacy wall. HIPAA laws may once have been adequate, but the circumstances have changed, and providers are no longer necessarily equipped to deal with ubiquitous technology, or regulatory loopholes. Providers' views may reflect experience with technology and state regulations that effectively limited interstate sharing. However, with the advent of interoperable health record systems, we now see states actively demanding access to such records for post-Roe enforcement purposes.

As a result, providers may find themselves unprepared for this new reality, where assumptions of privacy are increasingly in question.

4.3 Tensions and challenges providers face in protecting abortion seeking patients' privacy post-Roe

In this section, we first discuss the tensions and challenges that arise with current privacy protocols in the context of abortion scenarios, such as directing patients to abortion services in states where it remains legal, providing abortions to patients from states where it is illegal, and managing aftercare. While providers recognize these tensions and challenges, they are often unaware of the numerous risks posed to patients. In fact, our findings reveal that, in their efforts to comply with certain laws, clinics have unintentionally adopted insecure practices that introduce additional privacy liabilities for patients. We then examine the challenges providers face and their unmet needs regarding the process of offering privacy guidance to patients.

4.3.1 Finding an out-of-state abortion in states where abortion is illegal. Providers in states where abortion is banned reported that patients seeking out-of-state abortions may be referred by clinics in their home states. Clinics that support abortion rights in these states can direct patients to an abortion finder website or provide materials with the names and contact information of clinics in neighboring states.

A few providers in states where abortion is banned mentioned that when patients receive a positive pregnancy test, they are asked whether they plan to get an abortion. Providers may suggest that patients respond with "undecided" to deflect attention and reduce risks. Those who indicate they are "undecided" are given information about all options, including detailsabout clinics or a call center for referrals, without any decision being recorded in their medical records or insurance at that time. This practice also helps them avoid targeted misinformation or

discouraging outreach. One provider expressed concern about documenting discussions regarding abortion in medical records, particularly for patients on state insurance, noting that their clinic had previously received a letter from the state requesting medical records.

Patients who decide to cross state lines for an abortion are informed that they must book the appointment themselves, a measure intended to limit legal liability. Some providers express frustration that they cannot offer this assistance in this process, as doing so could be illegal.

> "I wish we could be able to help patients make appointments because we have the staff that's fully qualified to get the job done … we cannot do anything. So it's more of us standing on the outside looking in and we're like, 'Hey, we can only provide you with so many resources. It's just, you have to call … So [the clinic] limited us very, they give us a monthly allowance to help get these patients across state lines into a legal state. But I wish … that we can do more."

Therefore, in these initial communications, patients seeking out-of-state abortions typically make calls using a number provided by their home state clinic, clinic website, or even from a billboard. Alternatively, they may reach out via email.

Clinics that perform abortions may assist patients in securing funding for gas, transportation, hotels, and procedures. Patients typically arrange this funding through email and phone calls. However, at no point are patients advised to use burner phones or secure, encrypted messaging or email for these arrangements. Funding vouchers are often sent over insecure email, further exposing sensitive information to potential risks.

At the same time, while funding serves the practical purpose of defraying out-of-pocket costs, it also helps reduce the generation of records tied to abortion-seeking activity. For example, one provider in a state where abortion is legal explained that, for out-of-state patients who prefer not to use their insurance, funding can cover the costs of the procedure itself, not just the logistical expenses. This allows patients to avoid creating a financial trail tied to their insurance records.

> "But [legal state] made a counter-law or a counter-policy that says, we're not going to tell you anything. If they're coming in here for an abortion, … you have no way to request [patient records] from us. You are not going to penalize this person. So at least state-wise, we have policies in place to protect patients that are coming in from out of state … [If] they don't want it to be on their insurance record, like, at all. We can try to go find some funding for that and we specifically have one that just happened, I think, within the last year … Depending on their eligibility, it [this fund] will cover for half of whatever the abortion cost is, like just depending on the method and how far along they are."

Still, the reliance on insecure communication methods introduces a tension between providing financial support and ensuring adequate privacy protections.

4.3.2 Providing out-of-state abortion in states where it's legal. Providers in legal states report that once an out-of-state patient indicates their intent to receive abortion care at their clinic and confirms funding, communication predominantly takes place within their EHR message portal systems, rather than phone calls or email.

Some providers advise patients to set up a separate portal for direct communication with their clinic if they have privacy concerns. This ensures that abortion care remains distinct from their other medical records.

> "So usually, we interact with the patient in a secure chat that's inside of our electronic medical record … I tell patients some of the best ways if you feel like your phone or your computer is private is to have what's called MyChart, which is a patient portal that constantly communicates between you and the office."

> "Once they come in, they can set up a portal to send secure messages."

Many providers at clinics offeringabortions for out-of-state patients believe that their states' privacy laws protect EHRs from subpoenas or warrants. In some instances, specific clinics in certain states may refuse to comply and withstand legal challenges. However, many clinics routinely and legally share records across systems and providers, potentially exposing patients to prosecution in states where abortion is illegal.

Notably, a provider at one clinic that does not share records with other practices outside its facility indicated that patients choose to have procedures performed at their clinic specifically to ensure their medical records remain protected in a legal state, in casecomplications arise after they return home. Additionally, another provider mentioned that while their clinic offers confidential billing to out-of-state patients seeking abortions, some patients may go a step further in protecting their privacy by opting not to involve their insurance at all.

Even the few who do worry about sharing EHRs with other providers—and the possibility of patients' records being reported or forcibly released to authorities—believe that the release of these records is under the patient's control, even though this may not always be the case. As one provider noted:

"The only way that [EHRs] would make it there is if the patient decided to share that information with other providers through [EHR platform] or asked for a release of records."

This provider explained that when they see patients who have had abortions choosing to share their EHRs with other practices, they may confirm the decision and counsel them not to. However, it's not clear the extent to which patients are aware of this sharing and the counseling they receive about it.

Still, these instances highlight exceptions, rather than the rule. Providers generally do not view the records stored by their clinic as potential source of threats from law enforcement, and most express little concern about records being shared with other practices.

Notwithstanding those sporadic precautions and expressions of uneasiness, a more prevalent theme is a lack of clarity about when and how EHRs are shared and the potential risks that could expose patients to data breaches or prosecution. There is a reflexive impression, based on the habit and the presumptions of many years, that patients can generally rely on HIPAA to protect their EHRs. Providers, therefore, tend to view these precautions as exercises in diligence that may be seen as unnecessary. Providers are not fully convinced that additional precautions are necessary, believing that HIPAA protections are ultimately sufficient in the face of prosecutorial zeal. Their perspective also suggests that they do not incorporate the possibility of other healthcare providers accessing shared EHRs into their threat model.

4.3.3 Aftercare for out-of-state abortions. The primary concern with out-of-state abortions is aftercare, as it exposes patients to medical systems outside the provider's control in jurisdictions where abortion is illegal. Additionally, it may require patients make a long and potentially expensive journey back to a legal state for follow-up care. For this reason, providers prefer that patients be "complete"—meaning they have both the procedure and aftercare finished—before returning home.

> "So that's where we start. Let us do your follow-up. Let us make sure you're complete. And then after you're complete, you can go back to your doctor and the doctor doesn't have to [know]. It's up to you if you want to tell the doctor, but the doctor doesn't have to know that you went to have an abortion because it's not going to show. It doesn't say 'abortion' on your uterus."

Patients who receive out-of-state medication abortions often undergo some initial care in the state of the abortion provider. It is sometimes legally required for them to receive the medication abortion in that legal state, and it is certainly recommended that they remain there until the procedure is complete. This is primarily to mitigate the risk that minor complications or even routine symptoms could trigger medical intervention in a state where abortion is no longer legal.

However, when patients do return home before they are "complete," providers advise that if patients must return home before the abortion is complete, they should call the provider's clinic first if they experience concerning symptoms. This is especially important with medication abortions, where the risk of complications is exceedingly

low, but patients may experience incomplete abortions or become unnecessarily alarmed by symptoms and require reassurance.

> "We always say, if you're experiencing any symptoms, give us a call first."

Another risk that arises when patients are sent back to their home state with abortion medication pills is the possibility of mixing up their pills and taking them in the wrong sequence. This situation is not easily resolved in a state where abortion is illegal because patients have no recourse through established channels if they need help. They must either drive back for more pills or present to their local clinic or emergency room as if they are experiencing a miscarriage. Providers are confident that if patients do encounter complications, they are not obligated to disclose that they had a "medical abortion."

> "The patient needs to be in [legal state] and then to do a medication abortion, you also need to sign a form that says you're planning to take all the medication in [legal state]. And I got a call late in the night from this patient and she was in [illegal state] when she called and she had [a problem] ...In the old times, I would have said, that's no problem. Most likely it's going to work. [And if not,] just go to your local clinic, we'll send them a message, and you can pick up another dose of misoprostol there. But now, what we would have needed to do is either have her drive all the way back to [legal state] to pick up another dose, or her other option would be that we would not send any information at all to her local clinic ... [where she could go] and say, 'I think I might be miscarrying."'

> "I tell patients, there is no legal obligation to say medical abortion."

4.3.4 Provider counsel regarding technology privacy on personal devices. Providers rarely, if ever, offer patients guidance on how to protect their devices, despite having their own rules in place regarding personal devices at work to prevent access to patients' medical records. One provider noted that they believe their devices—and, consequently, their clinic's network—are more vulnerable when using social media or personal email. For this reason, their clinic discourages employees from using social media or personal email on clinic Wi-Fi.

Despite this awareness, providers are cautious about advising patients about how to manage privacy on their devices. While their goal is to ensure that patients are well-informed about their digital records and the associated risks, some say they emphasize the importance of respecting patients' autonomy. That notion is modeled along the lines of their approach to IPV, where they are trained to believe their role in protecting the safety and well-being of patients must be carefully balanced against the need to avoid behaviors that might challenge patient's agency or undermine rapport.

> "Well, it's really difficult because we, at least at my clinic, we're really, really serious about ... bodily autonomy almost, or making sure that we aren't making decisions for the patient almost ... So, especially when I'm concerned or if I'm worried maybe they aren't fully grasping this, I just almost reiterate myself ... I'm like, so when you go to your pediatrician, it's going to show that you had an appointment at this clinic, are you okay with that?"

Providers are often wary of giving advice because they may not fully understand the implications. Several recall that after Roe v. Wade was overturned, patients came to them with concerns about period-tracking apps; however, providers were hesitant to recommend deleting these apps due to their uncertainty about the associated risks. Beyond period tracking apps, which reached broader attention when Roe was overturned [85], providers note that it is actually rare for providers to hear the issue of device security raised by patients.

While a few providers note that patients occasionally mention turning off their GPS and deleting period tracking apps, these behaviors may not always be intended to prevent legal surveillance. An example is the concern a patient may have that their partner is tracking them, evidence of the way abortion and IPV risk can

potentially intersect. In all cases, providers say they do not advise patients, not necessarily because it's not their role, but simply that they do not have advice they feel is reliable to give.

> "There's nothing I think we've done to advise patients against turning off their phones and turning off GPS. Nothing I was ever told to do."

Regardless, beyond cautioning patients about certain obvious risks, providers keep advice to a minimum and avoid adopting an overbearing posture. Many providers do not recall actively seeking information about digital privacy related to abortion. While some have heard about period trackers and device security through social media platforms like TikTok, they are uncertain about the reliability of this information and do not feel qualified to verify it. Providers indicate a willingness to share digital privacy advice when they feel confident in its accuracy.

When it comes to EHRs, providers also acknowledge their limitations in offering advice beyond turning off sharing (among those who do) but do express a willingness—some even presume responsibility—to educate themselves and patients seeking abortions about the vulnerabilities that EHRs can pose.

> "They are at a much greater risk, and in an era where digital literacy isn't necessarily where it should be with all age groups and people from all backgrounds, that's something that needs to be shared, and it's our responsibility as healthcare providers to do that."

Notably, some providers believe that supporting privacy for out-of-state abortion patients falls within the jurisdiction of those assisting patients in navigating and accessing funding for abortion care across state lines. However, they are uncertain about what this guidance might entail or who is actually responsible for providing it.

> "Yeah, usually someone else tracks them more in-depth and communicates with them a little bit more until they get to the clinic or, you know, until they get to where they have to be just because there's other things that they consider, but I honestly don't know how they track that."

While some providers assume that the advice patients receive from those helping to navigate their out-of-state abortion may be technical, they elaborate on other types of guidance, for instance, the use of coded language.

> "I think that the person who would be the most helpful to have that conversation with actually would be our [patient advocate]. … We can get a patient connected to her, and she can go over their options in terms of how to find care or what words to use to get the care that she might need in her area … I don't know about technology. I think that's more she's saying when you walk into the emergency room, these are the words that you can say, or … In some places, if you use the word 'abortion' when you call … they'll refer you somewhere else. They won't see you. But if you call and say, 'I'm pregnant and I'm bleeding,' then they can see you."

As it happens, assumptions that privacy and technology counseling is occurring through the navigator function may be misplaced. We spoke with three people who help patients navigate out-of-state abortions, and they told us that they do not provide any privacy guidance about technology—even with regard to contacting the clinic or traveling out-of-state. As one such person states, if there were things to be concerned about with regard to privacy, they would be told:

> "And I'm almost sure if that's something that my boss was afraid of, she would have told us about that to let patients know, hey, to clear [browsing history] and do things like that."

4.3.5 Providers' perspectives on unmet privacy needs for patients receiving out-of-state abortions. Providers express a desire for more aftercare communication with out-of-state patients, with whom their digital interaction must be limited, and some have begun offering videos and pamphlets to address these treatment gaps.

Regarding technology, they want to understand what is unsafe so they can inform their patients accordingly. However, none of the providers could recall ever receiving or seeing any formal guidance for patients about device privacy.

5 DISCUSSION AND IMPLICATIONS

Without a doubt, providers view patient privacy counseling as a key responsibility, recognizing that privacy threats are proliferating and intensifying in a post-Roe environment, where reproductive health behaviors are being tracked and criminalized. However, it is less clear whether reproductive healthcare providers fully recognize the risks or are equipped to counsel patients about all the complex digital vectors of threat—some of which are new, some of which were previously present but never fully explored when the stakes seemed much lower. In the following sections, we will summarize the limitations of reproductive healthcare providers' threat models, discuss the potential role these providers could play as "privacy intermediaries," and highlight the importance of an expanded notion of informed consent alongside updated threat guidance.

5.1 The limits of reproductive healthcare providers' threat models

Providers currently focus on safeguarding patients' information from reaching their families, friends, or partners. However, this approach prioritizes protecting personal relationships, without fully considering how this information might be leveraged in legal actions for violating state laws—whether the threat originates from a family member, a hostile provider, or state authorities. Consequently, providers focus largely on their immediate environment and a set of foundational precautions, of which HIPAA is a key pillar. However, in these instances, HIPAA is seen as a critical barrier against threats, such as a partner finding out about a sexually transmitted disease, not against laws targeting abortions. Indeed, providers have been particularly sensitive to the special needs of certain categories of patients—minors, those receiving gender affirming care or with disapproving or abusive partners—against which HIPAA has been an effective defense.

When we asked about abortion-related threats concerning requests for patient medical records, providers seemed confident that they could defend against such requests, presuming their legal team could deflect them, regardless of the practical realities [59]. They also remain unaware of the increasing risk posed by interstate data flows through EHRs [143]. This lack of awareness is understandable, given that interstate legal frameworks are rapidly shifting underfoot, based on varying interpretations of the law and new legislation that incentivizes hostile healthcare providers to identify and report illegal abortions [46]. Indeed, there are numerous and varied efforts to reach across state lines to prosecute abortions [4, 38, 75, 78, 116].

Providers have long operated within a threat model shaped by limited and localized threats from parents and partners, and they now, understandably, face challenges in adapting to a more dangerous and dynamic landscape where abortion is criminalized. In the post-Roe era, the surface area of threat has expanded rapidly and dramatically—sometimes employing tactics previously tested on marginalized communities (e.g., [133]). These same tactics are now being appropriated for use in abortion contexts, where digital data can be easily targeted by authorities [35, 43].

Our interviews reveal that providers are not yet considering, nor do they have a clear view of, this broader landscape of threat (e.g., the risks associated with patients' abortion-related activities on their phones or EHRs). On the rare occasions when they are aware of patients' digital vulnerabilities, they do not feel equipped to provide meaningful guidance. However, because of their position in a patient's care network, providers are uniquely positioned to offer prescriptive advice regarding patients' digital data and take steps to protect their EHRs.

5.2 Imagining reproductive healthcare providers as privacy intermediaries

McDonald and Andalibi envision a role for reproductive healthcare providers as privacy intermediaries who offer "holistic and integrative privacy management" for those made vulnerable by the laws in their state [85]. In our interviews, providers demonstrated a highly nuanced approach to providing privacy protections to certain categories of vulnerable patients. Here we discuss their existing roles as privacy intermediaries and how they are, in theory, well positioned to provide digital privacy guidance related to abortions, but are not currently equipped to do so by virtue of their limited sightline on a more broadly threatening environment. This presents a significant challenge for providers who may excel at threat modeling around traditional risks but lack training in technology as it pertains to the port-*Roe* surveillance landscape.

Reproductive healthcare providers have long been in a position of helping patients navigate personal privacy in hostile or abusive environments. EHRs have historically been well understood to provide protection against local and personal threats (family, partners, employers, associates who cannot (legally or easily) but not as much with more nebulous threats from government and law enforcement. We have learned that reproductive healthcare providers are, in fact, quite practiced at thwarting disapproving and abusive partners and family. Even while few of these providers were attuned to the potential risks of sharing EHRs across state lines, or EHRs on patient devices, they nevertheless were diligent and astute observers of patients' lives, and adept students of the dynamics and risks relevant to their patients' healthcare needs—whether birth control, abortion, or gender affirming care. Those already attuned to the risks of sharing EHRs have protocols in place to screen for EHR preferences, review communication procedures, create passcodes, and restrict information flows through billing—in other words, an intricate apparatus of consent pertaining to known, personal adversaries.

It seems clear that reproductive healthcare providers are well positioned to evaluate patients' situations, ask pertinent questions, and provide guidance on how to manage their digital privacy and health records. However, in this new environment, there is also a pressing need to help providers integrate their knowledge of patient care with a nuanced understanding of interstate legal threats and their own engagement with them. This integration may require providers to more deeply consider their ethical responsibility regarding record maintenance for patients who they know will be crossing state lines. While well situated to help, reproductive healthcare providers do not currently have a legal obligation to inform patients about their digital privacy risks, and that issue too must be resolved in order for patients to receive the benefit of holistic standard privacy care.

5.3 Updating the concept of informed consent

For informed consent to be *fully* achieved in reproductive healthcare settings, it is crucial that patients, *as part of the informed consent process*, understand their data flows, the types of threats to data privacy that exist, who has potential access to their data, and what specific information can be obtained. To achieve this, reproductive healthcare providers need to have the necessary knowledge and tools necessary to provide patients with accurate information, enabling them to make truly informed choices about managing their reproductive healthcare data.

It stands to reason that patients can appreciate the nuances that make their EHR data—or any information about their abortion—a potential threat in the hands of hostile healthcare providers, family members, or law enforcement. Indeed, literature examining patients' communications with healthcare providers has shown that patients can play an active role in managing their data [61]. Providers reported that patients who conceal their sexual orientation or gender-affirming care from family members, as well as younger clients hiding their sexual activity, are often well-versed in the complexities of data flows. This is likely due to the tangible threats they face; their concerns are *not at all* abstract but vivid and concrete because they are local and immediate. In contrast, abortion-seeking patients may not have as much experience with these risks, as their need for an abortion is circumstantial rather than rooted in a persistent, identity-based vulnerability. To the extent that an updated notion of informed consent requires clarity on how law enforcement can access data beyond EHRs, patients who

are not experienced in managing such threats will need encouragement to think more actively about their data and vulnerabilities—similar to how reproductive healthcare providers note that their traditionally vulnerable patients (e.g., LGBTQ+, minors, IPV survivors) often do.

Research has shown that subtle changes in format and delivery can significantly influence how patients are sensitized to and think about informed consent in the realm of digital privacy protection [130]. One approach could be to develop contextual guidance—such as by assisting reproductive healthcare providers in informing patients about data flows during the setup of patient portals, reviewing medical histories that generate EHRs, and explaining the limitations of HIPAA when accessing medical data on personal devices. While the providers we spoke with made some relevant gestures in that direction—such as reminding patients that their passwords should not be easily guessed by family members and having them sign releases to upload their medical information to the portal—these reminders are narrowly framed and fail to address the broader risks of digital threats that patients may face.

Additionally, reproductive healthcare providers can initiate conversations with patients about how they use their devices and the associated risks, especially in relation to the people in their lives and the laws in their state. Providers should adopt the practices of the few we spoke with who explain EHR data flows before asking patients whether they wish to share their information. While reproductive healthcare providers routinely navigate the complexities of their patients' circumstances, they need support to acquire an updated understanding of the broader and more intricate threat model than their experience has prepared them for. Finally, while providers are already over-burdened [110], we see no way around the need to update how informed consent is conceptualized and achieved post-Roe.

6 RECOMMENDATIONS AND DIRECTIONS FOR FUTURE WORK

Based on our findings of providers' practices and understandings, we provide preliminary privacy guidance for reproductive healthcare providers to better protect their patients data and digital privacy.

EHR guidance. There is reason to believe that once EHRs cross state lines [4, 38, 74, 75, 78, 143] or end up on patients' personal devices [41, 107], they become threats to both patients and reproductive healthcare providers. Some types of advice that need to be further explored are:

- Give reproductive healthcare providers a basic understanding of the typical EHR information flow threats [41, 92] and what *their clinic* EHR system does (e.g., sharing defaults, segmentation [41]), which most providers didn't know. Inform reproductive providers about the state laws that impact them and their patients, with ongoing guidance about how states are attempting to further test HIPAA laws (e.g., [4, 38, 75, 78]) and what the implications might be for their clinic.
- Inform reproductive healthcare providers that EHR storage, as well as communications about care that takes place in EHRs, may not be protected by HIPAA under several circumstances: when stored on patients' devices [107], when shared with apps not protected by HIPAA [53, 59, 105], when practices/physicians are subpoenaed [106, 109], and when shared across state lines [41, 143]. Guidance should be given for each of these threats.
- Provide guidance for talking to patients about, e.g., how EHR distribution works and the best plan for sharing across healthcare providers. If the goal is to coordinate and communicate aftercare with patients rather than transfer records, then limited record-keeping may be sufficient for out-of-state patients.
- Clinics vary in their protocols for sharing health data, so before seeking abortion care, patients should be given a set of questions to ask potential out-of-state healthcare providers about how they communicate and store EHRs and to discuss options for alternatives, promoting informed consent.

Patient device guidance. Authorities do not need access to EHRs from healthcare providers to start an investigation [35, 112]. Hostile healthcare providers [71], friends, family, and partners [84] can report on those they suspect of receiving an abortion [59], which allows law enforcement to seize individuals' devices [112]. Patients' phones generate a tremendous trove of data [28], including texts, social media, search histories, location data, purchasing histories, and health apps [43, 124]. But law enforcement can cast wider nets through geofencing [25, 45], keyword warrants [35, 126] or simply through access to third parties [35, 129] to identify patients who go to clinics [25, 131] or perform other abortion related activities online, including visits to clinic websites for scheduling (e.g., [68]), searches (e.g., [111]) and visits to abortion pill websites (e.g., [63, 72]). Some types of information and advice for patients that need to be further explored are:

- Searches for and visits to abortion pill and clinic websites can be tracked [63, 72, 111] by third parties like Google, Meta, and TikTok [68] and thus accessed by law enforcement [98].
- Phones can be used to track visits to a physical clinic [25, 45, 131].
- Communications on social media and messaging apps (e.g., [70]), browsing histories, location, and payments can be investigated if suspected of an abortion [43, 112, 124]. Devices can be seized and subpoenas or warrants can be issued to the companies that collect information related to abortion [10, 72, 98, 111].
- Other methods of surveillance outside of device location tracking include video cameras when making purchases in stores, tolls, and license plate photos and scanners [36, 37].
- HIPAA does not protect health-related information that is not stored in EHRs (e.g., [99] and EHRs may not be protected in hostile states (e.g., [41, 75, 78, 143]).
- It is important to understand the privacy practices of health and period tracking apps [43, 117, 139].
- Compartmentalizing daily activities from abortion-related actions can help maintain privacy, as recommended by the EFF [19, 20].

Future work will build upon and refine these suggestions, along with the threat model data flow we have presented, to create an accessible and effective guide or toolkit for reproductive healthcare providers. These models must be continually updated for accuracy and emphasis to reflect changes in the interpretation of laws through litigation and prosecution. We are only beginning to understand the limitations of what HIPAA does not cover in this digital era [59, 99], a challenge even those responsible for enforcing it are struggling to clarify [109].

7 CONCLUSIONS

Providers primarily focus on safeguarding patients' information within the physical spaces where they deliver care and managing electronic health record (EHR) information flows to family members or partners, particularly for vulnerable patient groups such as minors, individuals receiving gender affirming care, and those with disapproving or abusive partners. However, providers do not fully grasp the complex digital landscape of threats that abortion patients face from all sides. While EHRs may be vulnerable to both hostile providers and governments, social media, third-party platforms, and patient devices also remain susceptible to government access. As a result, these digital threats are not necessarily prioritized in providers' privacy concerns. This is partly because their threat models have not been tested or updated to account for state-level adversaries, whose digital reach almost certainly bypasses health privacy laws. Furthermore, providers are driven by their responsibility to lower barriers to care for their patients. Against this background, we provide preliminary guidance for providers to inform their patients about the limits of HIPAA as it pertains to EHRs and the security risks of their digital activities and devices, while empowering them to access the healthcare they need.

8 ACKNOWLEDGMENTS

This work was supported by the National Science Foundation Grant no: 2309275, 2309277, 2309278.

REFERENCES

[1] 2021. Standard Technology Presents Opportunities for Medical Record Data Extraction. *Pew* (2021). https://pew.org/2LSl3Xk

[2] 2022. *Better protection from invasive data requests for victims of rape.* https://www.gov.uk/government/news/better-protection-from-invasive-data-requests-for-victims-of-rape

[3] 2022. *Washington D.C. B24-0808 | 2021-2022 | 24th Council.* https://legiscan.com/DC/bill/B24-0808/2021

[4] 2023. 19 GOP Attorneys General Seek Private Medical Records of Patients Who Obtain Out-of-State Abortions. https://www.democracynow.org/2023/7/25/tamarra_wieder_abortion_rights_planned_parenthood

[5] 2023. *Abortion Laws by State.* https://reproductiverights.org/maps/abortion-laws-by-state/

[6] 2023. Governor Moore Signs Historic Reproductive Freedom Legislation, Protects Women's Reproductive Rights In Maryland - Press Releases - News - Office of Governor Wes Moore. https://governor.maryland.gov/news/press/pages/Governor-Moore-Signs-Historic-Reproductive-Freedom-Legislation,-Protects-Women%E2%80%99s-Reproductive-Rights-In-Maryland.aspx.

[7] 2023. *open.epic :: Interoperability Guide.* https://open.epic.com/Home/InteroperabilityGuide?whoAmI=patient&whatIWant=getHealthRecord

[8] 2024. OCR Finalizes HIPAA Modifications to Strengthen Reproductive Health Care Privacy. https://www.crowell.com/en/insights/client-alerts/ocr-finalizes-hipaa-modifications-to-strengthen-reproductive-health-care-privacy.

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

[10] Bobby Allyn. 2022. Privacy advocates fear Google will be used to prosecute abortion seekers. (2022). https://www.npr.org/2022/07/11/1110391316/google-data-abortion-prosecutions

[11] Teresa Almeida, Laura Shipp, Maryam Mehrnezhad, and Ehsan Toreini. 2022. Bodies Like Yours: Enquiring Data Privacy in FemTech. In *Adjunct Proceedings of the 2022 Nordic Human-Computer Interaction Conference (NordiCHI '22)*. Association for Computing Machinery, 1–5. https://doi.org/10.1145/3547522.3547674 Place: New York, NY, USA.

[12] Nazanin Andalibi. 2020. Disclosure, Privacy, and Stigma on Social Media: Examining Non-Disclosure of Distressing Experiences. 27, 3 (2020), 18:1–18:43. https://doi.org/10.1145/3386600

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

[14] Nazanin Andalibi, Margaret E. Morris, and Andrea Forte. 2018. Testing Waters, Sending Clues: Indirect Disclosures of Socially Stigmatized Experiences on Social Media. 2 (2018), 19:1–19:23. Issue CSCW. https://doi.org/10.1145/3274288

[15] Nazanin Andalibi, Pinar Ozturk, and Andrea Forte. 2017. Sensitive Self- disclosures, Responses, and Social Support on Instagram: the Case of #Depression.

[16] Julie Appleby. 2022. Three things to know about health insurance coverage for abortion. (2022). https://www.npr.org/sections/health-shots/2022/07/13/1111078951/health-insurance-abortion

[17] Brianna Bailey. 2023. An Oklahoma Mom's Court Challenge Seeks to End Charges for Pregnant Women Who Use Medical Marijuana. *The Frontier* (2023).

[18] Robert Baldwin III. 2022. Losing a pregnancy could land you in jail in post-Roe America. (2022). https://www.npr.org/2022/07/03/1109015302/abortion-prosecuting-pregnancy-loss

[19] Daly Barnett. 2022. *Digital Security and Privacy Tips for Those Involved in Abortion Access.* https://www.eff.org/deeplinks/2022/05/digital-security-and-privacy-tips-those-involved-abortion-access

[20] Daly Barnett. 2022. *Security and Privacy Tips for People Seeking An Abortion.* https://www.eff.org/deeplinks/2022/06/security-and-privacy-tips-people-seeking-abortion

[21] Kristen Barta, Cassidy Pyle, and Nazanin Andalibi. 2023. Toward a Feminist Social Media Vulnerability Taxonomy. 7 (2023), 100:1–100:37. Issue CSCW1. https://doi.org/10.1145/3579533

[22] Emily Bazelon. 2022. Risking Everything to Offer Abortions Across State Lines. (2022). https://www.nytimes.com/2022/10/04/magazine/abortion-interstate-travel-post-roe.html

[23] Lydia A. Bazzano, Jaquail Durant, and Paula Rhode Brantley. 2021. A Modern History of Informed Consent and the Role of Key Information. 21, 1 (2021), 81–85. https://doi.org/10.31486/toj.19.0105

[24] Johana Bhuiyan. 2022. How can US law enforcement agencies access your data? Let's count the ways. (2022). https://www.theguardian.com/technology/2022/apr/04/us-law-enforcement-agencies-access-your-data-apple-meta

[25] Johana Bhuiyan. 2023. Health data privacy post-Roe: can our information be used against us? (2023). https://www.theguardian.com/us-news/2023/jun/24/health-data-privacy-protection-roe-abortion-tech-laws

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

[27] Shannon Bond. [n. d.]. Lyft And Uber Will Pay Drivers' Legal Fees If They're Sued Under Texas Abortion Law. ([n. d.]). https://www.npr.org/2021/09/03/1034140480/lyft-and-uber-will-pay-drivers-legal-fees-if-theyre-sued-under-texas-abortion-la

[28] Eric Boodman, Tara Bannow, Bob Herman, and Casey Ross. 2022. *HIPAA won't protect you if prosecutors want your reproductive health records.* https://www.statnews.com/2022/06/24/hipaa-wont-protect-you-if-prosecutors-want-your-reproductive-health-records/

[29] Emma Bowman. 2022. As states ban abortion, the Texas bounty law offers a way to survive legal challenges. (2022). https://www.npr.org/2022/07/11/1107741175/texas-abortion-bounty-law

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

[31] Virginia Braun and Victoria Clarke. 2019. Reflecting on reflexive thematic analysis. 11, 4 (2019), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

[32] Virginia Braun, Victoria Clarke, Nikki Hayfield, and Gareth Terry. 2018. Thematic Analysis. In *Handbook of Research Methods in Health Social Sciences*, Pranee Liamputtong (Ed.). Springer, 1–18. https://doi.org/10.1007/978-981-10-2779-6_103-1

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

[34] Lynda C Burton, Gerard F Anderson, and Irvin W Kues. 2004. Using Electronic Health Records to Help Coordinate Care. *The Milbank Quarterly* 82, 3 (Sept. 2004), 457–481. https://doi.org/10.1111/j.0887-378X.2004.00318.x

[35] Sophie Bushwick. 2022. Yes, Phones Can Reveal if Someone Gets an Abortion. (2022). https://www.scientificamerican.com/article/yes-phones-can-reveal-if-someone-gets-an-abortion/

[36] Nick Hidalgo Cagle, Matt. 2024. *Dozens of Police Agencies in California Are Still Sharing Driver Locations with Anti-Abortion States. We're Fighting Back. \textbar ACLU.* https://www.aclu.org/news/privacy-technology/dozens-of-police-agencies-in-california-are-still-sharing-driver-locations-with-anti-abortion-states-were-fighting-back

[37] Albert Fox Cahn and Eleni Manis. 2022. Pregnancy Panopticon: Abortion Surveillance After Roe. https://www.stopspying.org/pregnancy-panopticon

[38] David W. Chen. 2023. Idaho Bans Out-of-State Abortions for Minors Without Parent's Consent. (2023). https://www.nytimes.com/2023/04/05/us/idaho-out-of-state-abortions-minors-ban.html

[39] Rebecca Chowdhury. 2022. *High-Tech Surveillance Could Track Abortion-Seekers in U.S.* https://time.com/6184111/abortion-surveillance-tech-tracking/

[40] Chia-Fang Chung, Kristin Dew, Allison Cole, Jasmine Zia, James Fogarty, Julie A. Kientz, and Sean A. Munson. 2016. Boundary Negotiating Artifacts in Personal Informatics: Patient-Provider Collaboration with Patient-Generated Data. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. Association for Computing Machinery, 770–786. https://doi.org/10.1145/2818048.2819926 Place: New York, NY, USA.

[41] Ellen Wright Clayton, Peter J Embí, and Bradley A Malin. 2023. Dobbs and the future of health data privacy for patients and healthcare organizations. 30, 1 (2023), 155–160. https://doi.org/10.1093/jamia/ocac155

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

[43] Cynthia Conti-Cook. 2020. Surveilling the Digital Abortion Diary. 50, 1 (2020). https://scholarworks.law.ubalt.edu/ublr/vol50/iss1/2

[44] David Cox. 2024. 'They thought they were doing good but it made people worse': why mental health apps are under scrutiny. (2024). https://www.theguardian.com/society/2024/feb/04/they-thought-they-were-doing-good-but-it-made-people-worse-why-mental-health-apps-are-under-scrutiny

[45] Joseph Cox. 2022. *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics.* https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood

[46] James Dawson. 2023. Idaho lawmakers pass a bill to prevent minors from leaving the state for abortion. (2023). https://www.npr.org/2023/03/30/1167195255/idaho-trafficking-abortion-minors-interstate-travel-criminalize

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

[48] Ashley Emery. 2024. *Data Privacy & Reproductive Freedom.* Technical Report. national insistute for women and families.

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

[50] CT Mirror Explains. 2022. CT is now an abortion 'safe harbor.' What does that mean? (2022). http://ctmirror.org/2022/06/27/ct-will-become-a-safe-harbor-for-abortion-seekers-on-july-1-what-does-that-mean/

[51] Nir Eyal. 2014. Using informed consent to save trust. 40, 7 (2014), 437–444. https://doi.org/10.1136/medethics-2012-100490

[52] Andrea Forte, Nazanin Andalibi, and Rachel Greenstadt. 2017. Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians.

[53] Geoffrey A. Fowler. 2019. Help Desk: Can your medical records become marketing? We investigate a reader's suspicious 'patient portal.'. (2019). https://www.washingtonpost.com/technology/2019/10/22/help-desk-can-your-medical-records-become-marketing-we-investigate-readers-suspicious-patient-portal/

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

[55] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. 1 (2017), 46:1–46:22. Issue CSCW. https://doi.org/10.1145/3134681

[56] Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syed Asad Naqvi. 2019. The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. 45, 5 (2019), 521–536. https://doi.org/10.1109/TSE.2017.2782813

[57] Gennie Gebhart. 2019. *EFF's Recommendations for Consumer Data Privacy Laws.* https://www.eff.org/deeplinks/2019/06/effs-recommendations-consumer-data-privacy-laws

[58] Office of the Attorney General. 2023. *Protecting Washingtonians' Personal Health Data and Privacy.* https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy

[59] Thomas Germain. 2022. Guess What? HIPAA Isn't a Medical Privacy Law. (2022). https://www.consumerreports.org/health/health-privacy/guess-what-hipaa-isnt-a-medical-privacy-law-a2469399940/

[60] Stephen B. Wicker Ghosh, Dipayan. 2020. *Reading in the Panopticon: Your Kindle May Be Spying on You, But You Can't Be Sure.* https://cacm.acm.org/magazines/2020/5/244335-reading-in-the-panopticon/abstract

[61] Rose M Gilbert, Dayyanah Sumodhee, Nikolas Pontikos, Catherine Hollyhead, Angus Patrick, Samuel Scarles, Sabrina Van Der Smissen, Rodrigo M Young, Nick Nettleton, Andrew R Webster, and Jocelyn Cammack. 2022. Collaborative Research and Development of a Novel, Patient-Centered Digital Platform (MyEyeSite) for Rare Inherited Retinal Disease Data: Acceptability and Feasibility Study. 6, 1 (2022), e21341. https://doi.org/10.2196/21341

[62] Michelle Goldberg. 2021. When a Miscarriage Is Manslaughter. (2021). https://www.nytimes.com/2021/10/18/opinion/poolaw-miscarriage.html

[63] Jennifer Gollan. 2023. *Websites Selling Abortion Pills Are Sharing Sensitive Data With Google.* https://www.propublica.org/article/websites-selling-abortion-pills-share-sensitive-data-with-google

[64] Michele Goodwin. 2020. *Policing the Womb: Invisible Women and the Criminalization of Motherhood.* Cambridge University Press.

[65] Karen Gullo. 2024. Location Data Tracks Abortion Clinic Visits. Here's What to Know. *Electronic Frontier Foundation* (March 2024). https://www.eff.org/deeplinks/2024/03/location-data-tracks-abortion-clinic-visits-heres-what-know

[66] David A Haggstrom and Thomas Carr. 2022. Uses of Personal Health Records for Communication Among Colorectal Cancer Survivors, Caregivers, and Providers: Interview and Observational Study in a Human-Computer Interaction Laboratory. 9, 1 (2022), e16447. https://doi.org/10.2196/16447

[67] Grace E. Howard. 2024. *The Pregnancy Police: Conceiving Crime, Arresting Personhood.*

[68] Tatum Hunter. 2022. You scheduled an abortion. Planned Parenthood's website could tell Facebook. (2022). https://www.washingtonpost.com/technology/2022/06/29/planned-parenthood-privacy/ Section: Your Data and Privacy.

[69] Marisa Iati. 2022. Pregnant women were jailed over drug use to protect fetuses, county says. (2022). https://www.washingtonpost.com/nation/2022/09/08/pregnant-women-drugs-jail/

[70] Martin Kaste. 2022. Nebraska cops used Facebook messages to investigate an alleged illegal abortion. (2022). https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion

[71] Parvaja S. Kavattur, Somjen Frazer, El-Shafei, Laura Laderman, Lindsey Hull, Walter-Johnson Fikayo, Sana Sussman, and Lynn M. Paltrow. 2024. The Rise of Pregnancy Criminalization: A Pregnancy Justice Report. https://www.pregnancyjusticeus.org/rise-of-pregnancy-criminalization-report/

[72] Jon Keegan and Dara Kerr. 2022. Online Abortion Pill Provider Hey Jane Used Tracking Tools That Sent Visitor Data to Meta, Google, and Others – The Markup. (2022). https://themarkup.org/pixel-hunt/2022/07/01/online-abortion-pill-provider-hey-jane-used-tracking-tools-that-sent-visitor-data-to-meta-google-and-others

[73] Bridget G. Kelly and Maniza Habib. 2024. Missed period? The significance of period-tracking applications in a post-Roe America. 31, 4 (2024), 2238940. https://doi.org/10.1080/26410397.2023.2238940

[74] Raman R Khanna, Sara G Murray, Timothy Wen, Kirsten Salmeen, Tushani Illangasekare, Nerys Benfield, Julia Adler-Milstein, and Lucia Savage. 2022. Protecting reproductive health information in the post-Roe era: interoperability strategies for healthcare institutions. *Journal of the American Medical Informatics Association : JAMIA* 30, 1 (Oct. 2022), 161–166. https://doi.org/10.1093/jamia/ocac194

[75] Eleanor Klibanoff and William Melhado. 2024. Texas conservatives test how far they can extend abortion and gender-transition restrictions beyond state lines. (2024). https://www.texastribune.org/2024/02/09/texas-abortion-transgender-care-outside-state-borders/

[76] Loren Kohnfelder and Praerit Garg. 1999. The threats to our products. https://shostack.org/files/microsoft/The-Threats-To-Our-Products.docx.

[77] Sam Levin. 2022. She was jailed for losing a pregnancy. Her nightmare could become more common. (2022). https://www.theguardian.com/us-news/2022/jun/03/california-stillborn-prosecution-roe-v-wade

[78] Ray Lewis. 2024. 16 AGs threaten Maine over bill impacting 'gender transition surgeries for children'. (2024). https://wpde.com/amp/news/nation-world/16-ags-threaten-maine-over-bill-impacting-gender-transition-surgeries-for-children-attorneys-general-texas-florida-kentucky-tennessee-and-west-virginia-ld-227-anna-perry-lisa-keim-gender-lgbtq-transgender
[79] Ron Lieber and Tara Siegel Bernard. 2022. Payment Data Could Become Evidence of Abortion, Now Illegal in Some States. (2022). https://www.nytimes.com/2022/06/29/business/payment-data-abortion-evidence.html
[80] Alan F. Luo, Noel Warford, Samuel Dooley, Rachel Greenstadt, Michelle L. Mazurek, and Nora McDonald. 2023. How Library IT Staff Navigate Privacy and Security Challenges and Responsibilities. (2023). https://osf.io/f589r/
[81] Shefali Luthra. 2023. *Could Facebook messages be used in abortion-related prosecution?* https://19thnews.org/2023/07/abortion-laws-facebook-messages-digital-privacy/
[82] Kenneth D. Mandl and Eric D. Perakslis. 2021. HIPAA and the Leak of "Deidentified" EHR Data. 384, 23 (2021), 2171–2173. https://doi.org/10.1056/NEJMp2102616
[83] Nina Martin. 2014. *A Stillborn Child, A Charge of Murder and the Disputed Case Law on 'Fetal Harm'.* https://www.propublica.org/article/stillborn-child-charge-of-murder-and-disputed-case-law-on-fetal-harm
[84] Sarah McCammon. 2023. Texas man sues ex-wife's friends for allegedly helping her get abortion pills. (2023). https://www.npr.org/2023/03/11/1162805773/texas-man-sues-abortion-pills
[85] Nora McDonald and Nazanin Andalibi. 2023. "I Did Watch 'The Handmaid's Tale'": Threat Modeling Privacy Post-Roe in the United States. (2023).
[86] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020-04-21). Association for Computing Machinery, 1–14. https://doi.org/10.1145/3313831.3376167 Place: New York, NY, USA.
[87] Nora McDonald and Andrea Forte. 2021. Powerful Privacy Norms in Social Network Discourse. 5, 2 (2021).
[88] Nora McDonald and Andrea Forte. 2022. Privacy and Vulnerable Populations. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer International Publishing, 337–363. https://doi.org/10.1007/978-3-030-82786-1_15
[89] Nora McDonald, Rachel Greenstadt, and Andrea Forte. 2023. Intersectional Thinking about PETs: A Study of Library Privacy. 2023 (2023), 480–495. https://doi.org/10.56553/popets-2023-0064
[90] Maryam Mehrnezhad and Teresa Almeida. 2021. Caring for Intimate Data in Fertility Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, 1–11. https://doi.org/10.1145/3411764.3445132 Place: New York, NY, USA.
[91] Kelcie Moseley-Morris. 2023. *Idaho Supreme Court upholds abortion ban, civil enforcement law • Idaho Capital Sun.* https://idahocapitalsun.com/2023/01/05/idaho-supreme-court-upholds-abortion-ban-civil-enforcement-law/
[92] Vivian Genaro Motti and Shlomo Berkovsky. 2022. Healthcare Privacy. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer International Publishing. https://doi.org/10.1007/978-3-030-82786-1
[93] Suvda Myagmar, Adam J. Lee, and William Yurcik. 2005. Threat modeling as a basis for security requirements. In *StorageSS '05: Proceedings of the 2005 ACM workshop on Storage security and survivability.*
[94] Arvind Narayanan and Vitaly Shmatikov. 2007. How To Break Anonymity of the Netflix Prize Dataset. https://doi.org/10.48550/arXiv.cs/0610105 arXiv:cs/0610105 Issue: arXiv:cs/0610105.
[95] Nicole Narea. 2022. *Why was a Texas woman charged with murder over an abortion?* https://www.vox.com/policy-and-politics/23021104/texas-abortion-murder-charge-starr-county
[96] Alfred Ng. 2024. *A company tracked visits to 600 Planned Parenthood locations for anti-abortion ads, senator says.* https://www.politico.com/news/2024/02/13/planned-parenthood-location-track-abortion-ads-00141172
[97] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. 79, 1 (2004), 101–139.
[98] Naomi Nix and Elizabeth Dwoskin. 2022. Search warrants for abortion data leave tech companies few options. (2022). https://www.washingtonpost.com/technology/2022/08/12/nebraska-abortion-case-facebook/
[99] Charles Ornstein. 2022. *Federal Patient Privacy Law Does Not Cover Most Period-Tracking Apps.* https://www.propublica.org/article/period-app-privacy-hipaa
[100] Justin Petelka, Lucy Van Kleunen, Liam Albright, Elizabeth Murnane, Stephen Voida, and Jaime Snyder. 2020. Being (In)Visible: Privacy, Transparency, and Disclosure in the Self-Management of Bipolar Disorder. 2020 (2020), 10.1145/3313831.3376573. https://doi.org/10.1145/3313831.3376573
[101] Tessa Pieper. 2023. *House passes bill that could establish Minnesota as a safe haven for reproductive health care - Session Daily - Minnesota House of Representatives.* https://www.house.mn.gov/SessionDaily/Story/17831
[102] Leslie J. Reagan. [n. d.]. *When Abortion Was a Crime: Women, Medicine, and Law in the United States, 1867-1973, with a New Preface.*
[103] Neil Richards and Woodrow Hartzog. 2018. The Pathologies of Digital Consent. 96 (2018), 1461. https://heinonline.org/HOL/Page?handle=hein.journals/walq96&id=1499&div=&collection=

[104] Office for Civil Rights (OCR). 2007. *When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials?* https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html
[105] Office for Civil Rights (OCR). 2019. *The access right, health apps, & APIs.* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html
[106] Office for Civil Rights (OCR). 2022. *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care.* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html
[107] Office for Civil Rights (OCR). 2022. *Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet.* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
[108] Office for Civil Rights (OCR). 2022. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates.* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html Last Modified: 2024-03-18T18:00:15-0400.
[109] Office for Civil Rights (OCR). 2023. *HIPAA Privacy Rule Notice of Proposed Rulemaking to Support Reproductive Health Care Privacy Fact Sheet.* https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/hipaa-reproductive-health-fact-sheet/index.html
[110] Erika L. Sabbath, Samantha M. McKetchnie, Kavita S. Arora, and Mara Buchbinder. 2024. US Obstetrician-Gynecologists' Perceived Impacts of Post–Dobbs v Jackson State Abortion Bans. *JAMA Network Open* 7, 1 (Jan. 2024), e2352109. https://doi.org/10.1001/jamanetworkopen.2023.52109
[111] Carolyn Said. 2022. *Searches for 'abortion pills' are spiking. Here's how Google could use your search history against you.* https://www.sfchronicle.com/tech/article/abortion-google-17275454.php
[112] Runa Sandvik. 2023. *How US police use digital data to prosecute abortions.* https://techcrunch.com/2023/01/27/digital-data-roe-wade-reproductive-privacy/
[113] Jayshree Sarathy, Sophia Song, Audrey Haque, Tania Schlatter, and Salil Vadhan. 2023. Don't Look at the Data! How Differential Privacy Reconfigures the Practices of Data Science. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, 1–19. https://doi.org/10.1145/3544548.3580791 Place: Hamburg Germany.
[114] Alfred Schutz. 1967. *The Phenomenology of the Social World.* Northwestern University Press.
[115] Carter Sherman. 2023. Idaho mother and son charged with kidnapping over out-of-state abortion. (2023). https://www.theguardian.com/us-news/2023/nov/01/idaho-mother-son-kidnap-charges-abortion
[116] Carter Sherman. 2023. Texas lawyer asks abortion funds for details of every procedure since 2021. (2023). https://www.theguardian.com/world/2023/sep/28/texas-lawyer-abortion-ban-procedure-patient-information
[117] Laura Shipp and Jorge Blasco. 2020. How private is your period?: A systematic analysis of menstrual app privacy policies. 2020, 4 (2020), 491–510. https://doi.org/10.2478/popets-2020-0083
[118] Evelyne Shuster. 1997. Fifty Years Later: The Significance of the Nuremberg Code. 337, 20 (1997), 1436–1440. https://doi.org/10.1056/NEJM199711133372006
[119] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. [n. d.]. Computer Security and Privacy for Refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)* (2018-05). 409–423. https://doi.org/10.1109/SP.2018.00023
[120] Molly Smith and Juno Mac. 2018. *Revolting Prostitutes: The Fight for Sex Workers' Rights.* Verso.
[121] Rock Stevens, Daniel Votipka, Elissa M. Redmiles, Colin Ahern, Patrick Sweeney, and Michelle L. Mazurek. 2018. The Battle for New York: A Case Study of Applied Digital Threat Modeling at the Enterprise Level. 621–637. https://www.usenix.org/conference/usenixsecurity18/presentation/stevens
[122] Frank Swiderski and Window Snyder. 2004. *Threat Modeling.* Microsoft Press.
[123] Paul Theurich, Josepha Witt, and Sebastian Richter. 2023. Practices and challenges of threat modelling in agile environments. 46, 4 (2023), 220–229. https://doi.org/10.1007/s00287-023-01549-5
[124] Jia Tolentino. 2022. We're Not Going Back to the Time Before Roe. We're Going Somewhere Worse. (2022). https://www.newyorker.com/magazine/2022/07/04/we-are-not-going-back-to-the-time-before-roe-we-are-going-somewhere-worse
[125] Emily Tseng, Rosanna Bellini, Yeuk-Yu Lee, Alana Ramjit, Thomas Ristenpart, and Nicola Dell. 2024. Data Stewardship in Clinical Computer Security:Balancing Benefit and Burden in Participatory Systems. *Computer Supported Cooperative Work* 8 (2024).
[126] Hayley Tsukayama. 2023. *A Year Since Dobbs, The Fight For Reproductive Privacy and Information Access Continues.* https://www.eff.org/deeplinks/2023/06/year-dobbs-fight-reproductive-privacy-and-information-access-continues
[127] Hayley Tsukayama. 2023. *A Year Since Dobbs, The Fight For Reproductive Privacy and Information Access Continues.* https://www.eff.org/deeplinks/2023/06/year-dobbs-fight-reproductive-privacy-and-information-access-continues
[128] Mary Tuma. 2023. The First "Wrongful Death" Case for Helping a Friend Get an Abortion. (2023). https://theintercept.com/2023/04/26/abortion-wrongful-death-texas-lawsuit/
[129] Remy Tumin. 2023. Pharmacies Shared Patient Records Without a Warrant, an Inquiry Finds. (2023). https://www.nytimes.com/2023/12/13/us/pharmacy-records-abortion-privacy.html
[130] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. Association

for Computing Machinery, 973–990. https://doi.org/10.1145/3319535.3354212 Place: New York, NY, USA.

[131] Alanna Vagianos. 2024. *Anti-Choice Group Tracked Planned Parenthood Visitors Using Phone Data.* https://www.huffpost.com/entry/anti-choice-group-targeted-planned-parenthood-visitors-using-phone-data_n_65ccf7dce4b0087d43c8b3a8

[132] Andrea Vittorio and Skye Witley. 2023. Abortion-Rights States Begin Shielding Digital Data Near Clinics. (2023). https://news.bloomberglaw.com/privacy-and-data-security/abortion-rights-states-begin-shielding-digital-data-near-clinics

[133] Nina Wang, Allison McDonald, Daniel Bateyko, and Emily Tucker. 2022. American Dragnet | Data-Driven Deportation in the 21st Century. *Center on Privacy & Technology at Georgetown Law* (2022).

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

[135] Mark Warner, Juan F. Maestre, Jo Gibbs, Chia-Fang Chung, and Ann Blandford. 2019. Signal Appropriation of Explicit HIV Status Disclosure Fields in Sex-Social Apps used by Gay and Bisexual Men. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19).* Association for Computing Machinery, 1–15. https://doi.org/10.1145/3290605.3300922 Place: New York, NY, USA.

[136] Gail Weiss, Gayle Salamon, Ann V. Murphy, Duane Davis, Lisa Guenther, Lewis R. Gordon, John D. Caputo, Kris Sealey, Mark Ralkowski, Natalie Cisneros, Kyle Whyte, Robert McRuer, George Yancy, Patricia Hill Collins, Rosalyn Diprose, Eduardo Mendieta, Alia Al-Saji, Charles W. Mills, Tamsin Kimoto, Debra Bergoffen, Shannon M. Mussett, Diane Perpich, Donald A. Landes, Ted Toadvine, Helen A. Fielding, Megan Burke, Mariana Ortega, David Morris, Moira Gatens, Dr Shiloh Whitney, Scott Marratto, Jenny Slatman, William McBride, Elena Ruiz, Rosemarie Garland-Thomson, Emily S. Lee, Lanei M. Rodemeyer, Joel Michael Reynolds, Shannon Sullivan, Jennifer McWeeny, Jack Reynolds, Linda Martin Alcoff, Lauren Guilmette, Sid Hansen, Axelle Karera, David Haekwon Kim, Keith Whitmoyer, Perry Zurn, Nancy J. Holland, Dorthea Olkowski, Talia Mae Bettcher, Kelly Oliver, Andrea Pitts, and Cynthia Willett. 2019. *50 Concepts for a Critical Phenomenology.* Northwestern University Press.

[137] Nicole Wetsman. 2022. *The fall of Roe v. Wade shows how little control patients have over medical records.* https://www.theverge.com/2022/6/29/23188211/medical-records-privacy-dobbs-roe

[138] Tracey A. Wilkinson. 2022. Dr. Caitlin Bernard Was Meant to Write This With Me Before She Was Attacked for Doing Her Job. (2022). https://www.nytimes.com/2022/07/15/opinion/doctors-roe-v-wade-ohio-10-year-old.html

[139] Jennifer Wright. 2019. The U.S. Is Tracking Migrant Girls' Periods to Stop Them From Getting Abortions. (2019). https://www.harpersbazaar.com/culture/politics/a26985261/trump-administration-abortion-period-tracking-migrant-women/

[140] Odette Yousef. 2024. How 'fetal personhood' in Alabama's IVF ruling evolved from fringe to mainstream. (2024). https://www.npr.org/2024/03/14/1238102768/fetal-personhood-alabama-ivf

[141] Cat Zakrzewski, Pransha Verma, and Claire Parker. 2022. Texts, web searches about abortion have been used to prosecute women. (2022). https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/

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

[143] Carleen Zubrzycki. 2022. The Abortion Interoperability Trap. *The Yale Law Journal Forum* 132 (Oct. 2022), 197–227. https://doi.org/10.2139/ssrn.4147900

Table 1. Detailed abortion data flow with scenarios, ranking of the status of threat and examples of sources used to evaluate the threats. Data flows are notated as **(Source) - (Target data) : (Method of obtaining data e.g., by what systems or services it is generated before it is subsequently given up, purchased, seized, etc.) > (Adversary/threat)**. In each flow, "generated" describes the data that results in the system or service in order for it to be accessed by prosecutors, e.g., through purchase or seizure via warrant, access to device during investigation, etc. The detailed data flows are merely examples and other iterations are possible. While not every component of the data flow is necessary, something must be generated and something must be obtained by prosecutors for it to be a threat. These scenarios are based on case law and legal theory cited in "source examples" and are not exhaustive. For instance, an implicit assumption for each of these scenarios is that prosecutors can always initiate warrants if they find out through friends, family, partner, or providers about suspected abortion.

Abortion data flow	Detailed data flow	Narrative illustrative example*	Status of threat	Source examples
Jane uses a period tracker	Patient (Pt) - menstrual data : Generated > period tracker App provider, data broker - menstrual data : Data purchase > Prosecutor Alternative (Alt): Patient phone - menstrual data : Seizure > Prosecutor	Police view unprotected menstrual health data from period tracking app companies or third parties that use their data to identify people like Jane who report lapses in their period.	experts have expressed concerns	[73, 139]
Jane buys a pregnancy test	Pt - Receipt : Generated > Online store Online store - Receipt : Warrant > Prosecutor Alt: Credit card company - Receipt : Warrant > Prosecutor	Jane buys a pregnancy test online. Police obtain purchase data as part of routine investigation.	data flow exists	[37]
	Pt - Surveillance footage : Video camera > Physical store Physical store - Video surveillance, receipt : Warrant > Prosecutor	Jane buys a pregnancy test (with cash) at her local pharmacy and is caught on video.	data flow exists	[39]
Jane gets a pregnancy test at the doctor	Pt - Abortion care record : Generated > Safe-state provider Safe-state provider - Abortion care record : EHR sharing > Illegal-state provider Illegal-state provider - Abortion care record : Disclosure > Prosecutor	Jane's abortion provider's records are seen by/shared with their provider in an illegal state and they report Jane to the police.	experts have expressed concern	[41, 143]
Jane uses health portal app with doctor to arrange abortion	Pt health app - Abortion care record : Generated > Safe-state provider Pt portal on phone - Abortion care record : Generated > Safe-state provider Pt health app - Abortion care record : Seizure > Prosecutor Pt portal on phone - Abortion care record : Seizure > Prosecutor	Jane arranges to have an abortion with an out-of-state provider. Police seize her phone in an investigation and review her healthcare app messages with her provider.	data flow exists	[107]
Jane brings her phone to an abortion clinic	Pt phone - Loc/nav data : Generated > Nav app Pt phone - Loc data : Generated > App with Loc services Pt phone - Loc/nav data : Seizure > Prosecutor Nav app, Loc services - Loc data : Data purchase, subpoena > Prosecutor	Jane goes to a clinic out-of-state for an abortion. She uses a navigation app to get there and/or opens up a random app on her phone along the way/outside the clinic.	experts have expressed concern	[45, 96, 131]
Jane drives to an abortion clinic	Patient (Pt) - License plate data : Generated > Traffic camera Traffic camera - License plate data : Direct access > Prosecutor	Jane drives to a clinic out-of-state and police surveillance captures her license plate.	experts have expressed concern	[36, 37]

Continued on next page

Table 1 – continued from previous page

Abortion data flow	Detailed data flow	Narrative illustrative example*	Status of threat	Source examples
Jane uses a rideshare app	Pt - Purchase history, nav data : Generated > Ride-share app Rideshare, third-parties - Purchase history, Loc data : Data purchase > Prosecutor	Jane takes a rideshare or rents a car to drive to the clinic where she gets an abortion.	Data flow exists	[27]
Jane searches/buys abortion pills online	Pt - Search history, browsing data : Generated > Browser Pt - Search history, browsing data : Generated > ISP ISP - Search for ”abortion pills” : Keyword warrant > Prosecutor	Police keyword warrants from Internet service providers (ISP) and tech companies like Google allow them to find people like Jane who are searching for ”abortion pills” and related keywords.	experts have expressed concern	[25, 35, 43, 111, 126]
	Pt - Search history, browsing data : Generated > Browser Pt - Search history, browsing data : Generated > ISP ISP - Search for ”abortion pills,” : Data purchase, subpoena > Prosecutor	During an investigation, police issue a subpoena to an ISP or purchase data to obtain records of Internet searches.	experts have expressed concern	[35, 98]
	Pt - Browsing data, email : Generated > Pt device Pt - Messages : Generated > Messaging app Pt device - Browsing data, email, messages : Seizure > Prosecutor	ER healthcare provider reports Jane to police when she shows up in the ER with suspected abortion. Police question Jane and obtain warrant for her phone. They review Jane’s internet browsing history and email confirming Jane bought abortion pills and texts with a friend discussing her abortion.	case law exists	[141]
	Pt - Miscarriage data : Generated > ER Pt - Search history : Generated > Browser Pt device - Search for ”buy abortion pills, etc.” : Disclosed willingly > Prosecutor	Jane reports miscarriage and is investigated. Jane voluntarily turns over her phone which shows she searched for “abortion pills.”	case law exists	[43]
	Pt - Browsing data : Generated > Third-party trackers Third-party trackers - Abortion pill site visit data : Data purchase > Prosecutors	Jane visits an online abortion pill provider and cookies alert Google, Meta and other third parties. Police in some states are purchasing these data and investigating patients.	experts have expressed concern	[63, 68, 72]

Continued on next page

Table 1 – continued from previous page

Abortion data flow	Detailed data flow	Narrative illustrative example*	Status of threat	Source examples
Jane has an abortion at a clinic/after care	Pt - Insurance records : Generated > Health insurance company Health insurance company - Insurance records : Warrant > Prosecutor	Jane goes to a legal state for an abortion and uses her health insurance to cover some of the cost. Prosecutors issues warrant to insurance company.	data flow exists	[16]
	Credit card company - Purchase data : Data purchase, subpoena > Prosecutor	Jane goes to a legal state for an abortion and pays with a credit card. Police issue a subpoena to credit card companies to view charges made to clinics for large amounts and find Jane.	experts have expressed concern	[79]
	Pt - Loc data : Generated > ISP ISP - Loc data : Geofence warrant > Prosecutor	Police issue geofencing warrant that allows them to see who has been with a certain distance of an abortion provider Jane visited for her abortion.	experts have expressed concern	[10, 25, 35]
	Pt health app - EHR : Seizure > Prosecutor Pt healthcare portal on phone - EHR : Seizure > Prosecutor Pt device - Search history, email, messages : Seizure > Prosecutor	Jane receives abortion medication at a clinic but continues to have bleeding. She goes to an ER in her state and tells providers she is having a miscarriage. This triggers investigation that results in warrant for her phone on which is found communications with providers and friends about her abortion.	experts have expressed concern, case law exists	[112, 141]
Jane talks about her abortion	Platform provider - Social media, msg. app messages : Warrant > Prosecutor	Police receive tip about an abortion from friends, family, or other and obtain warrant to gain access to Jane's Facebook account. They find texts in which she discusses her abortion on social media messaging apps, etc.	case law exists	[70, 81, 98]

Received 7 November 2023; revised 26 June 2024; accepted 26 September 2024