# The Chilling Effect of Dobbs: A Study of Mobile Health Apps Usage *

Naveen Basavaraj† Uttara M. Ananthakrishnan‡ Catherine Tucker§

November 6, 2024

**Abstract**

When the United States Supreme Court overturned Roe v. Wade in the landmark case of Dobbs v. Jackson Women's Health Organization, it brought significant changes to the landscape of reproductive rights and digital privacy. This study investigates how heightened concerns over government surveillance and data privacy, prompted by this ruling, affect the usage of digital health tracking tools among women. This paper uses a panel of mobile phone usage data to analyze user behavior before and after the Dobbs ruling leaked, focusing on app usage patterns. Our findings reveal a significant and chilling effect on the usage of mobile health apps. Specifically, we observe a 9.6% decrease in the weekly number of app usage sessions and a 31% reduction in average time spent on mobile health apps immediately after the Dobbs verdict leak. We observe that this reduction is even higher for FemTech apps — an 18.6% decline in the number of sessions and a 66.7% reduction in weekly time spent per week. We find that these effects are moderated by demographic factors like race, age, and income, as well as prior exposure to social media and news. Finally, we also observe the spillover effects of the decision in terms of increased adoption of privacy-preserving browsers following the leak.

**Keywords**: Abortion, Health Care, Apps, Privacy, Chilling Effect

**JEL Codes**: L86, M37, M38

*This research was generously funded by the International Center for Law & Economics (ICLE). This research was conducted independently without any oversight or editorial control.

†Heinz College of Information Systems and Public Policy, Carnegie Mellon University (naveentb@cmu.edu)

‡Heinz College of Information Systems and Public Policy, Carnegie Mellon University (uttara@cmu.edu)

§MIT Sloan School of Management, Massachusetts Institute of Technology (cetucker@mit.edu)

# 1 Introduction

The pervasive use of smartphones around the world has contributed to a meteoric increase in the use of mobile health technologies in the last decade. Mobile health technologies have expanded from simply providing reminders and offering a way of communicating with healthcare providers to an umbrella term used to describe health and fitness apps, platform-based services, and wearable devices. Mobile health technologies have, therefore, ushered in a new era of quantified approaches to monitoring, self-management, and offering agency in managing health issues (Ghose et al., 2022; Chib and Lin, 2018). Pew Research found in 2020 that one in every five Americans was using a fitness tracker.[1] This shift is reinforced by a recent McKinsey survey of 5000 consumers that estimates the health and wellness market at $480 billion just in the U.S.[2] Although these changes were widespread across both men and women, studies and surveys find a higher adoption of healthcare technology among women. McKinsey describes the 'FemTech' market – the mobile healthcare technology that helps address women-specific healthcare concerns including menstruation, ovulation, and fertility – to be between $500 million and $1 billion.[3] Another report by MStudies estimates that more than 50 million women use FemTech apps (Worsfold et al., 2021). Despite the ubiquitous adoption of mobile healthcare technologies and the benefits they confer on users, there are significant concerns among the users of these apps about how personal health data are collected, shared and used by apps (Liu et al., 2022; Hutton et al., 2018; Shipp and Blasco, 2020; Mehrnezhad et al., 2022; Guo et al., 2012), which can potentially lower the rate of adoption, particularly among vulnerable populations. In this paper, we study whether a perceived threat to digital data privacy can lead to chilling effects in the usage of

[1] https://www.pewresearch.org/short-reads/2020/01/09/about-one-in-five-americans-use-a-smart-watch-or-fitness-tracker/

[2] https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/the-trends-defining-the-1-point-8-trillion-dollar-global-wellness-market-in-2024

[3] https://www.mckinsey.com/industries/healthcare/our-insights/the-dawn-of-the-femtech-revolution

mobile health apps.

The benefits of healthcare app usage have been well documented in the medical and Information Systems literature (for a full review, see Rowland et al. (2020); Chib and Lin (2018); Liu and Willoughby (2018); Earle et al. (2020)). Studies in these fields find that healthcare apps are particularly useful for self-management of chronic diseases by tracking diet, activity, and personalized lifestyle recommendations. Prior studies in the literature on mobile health technology focused on improving clinical outcomes and creating a variety of techniques to encourage adoption and motivation through peers (Silveira et al., 2013), reminders (Liu and Willoughby, 2018), and personalization (Ghose et al., 2022). Barriers to entering the app development market are fairly low, which has led to an explosion in the number of available healthcare and fitness apps. Bates et al. (2018) estimate that there are more than 350,000 such apps available on the market, with high variability in quality, safety, and security. Governmental guidance and regulatory frameworks for data governance in this field are nascent and not comprehensive, with numerous and inconsistent evaluation frameworks (Bates et al., 2018; Ferretti et al., 2019; Hensher et al., 2021; Magrabi et al., 2019).

Data privacy concerns around mobile health technologies became particularly salient in the United States after the constitutional right to abortion was overturned in the 2022 Dobbs v. Jackson Women's Health Organization case. Following the historic ruling, abortion became severely restricted or outright banned in twenty-five states around the US. Although the ruling was primarily about access to reproductive health, digital data privacy became an important part of the conversation, with highly publicized reports of authorities in states with restrictive abortion laws using digital data to prosecute women (Shipp and Blasco, 2020; Baker-White and Emerson, 2022; McQuillan, 2022; Zakrzewski et al., 2022; Stopczynski, 2015; Gross, 2024; Wright and Vazquez, 2022; Hill, 2022; Conti-Cook, 2020; Murphy, 2022; Joh, 2022; Carr Smyth, 2023). These reports prompted nationwide debates, both from the

public and lawmakers, on the issues of digital privacy and the governmental authority to access digital records of personal information, which can then be used to implicate users in criminal proceedings. This paper studies whether the threat of surveillance of women's reproductive health deters users, and particularly women, from adopting and using mobile health apps.

The empirical effects of restrictive laws are not entirely clear for the following reasons. Theoretically, there could be no change in the usage of mobile health and FemTech apps due to the passage of restrictive laws around abortion. Though there was extensive media coverage making data privacy on mobile health apps salient, the awareness of such concerns among the general population could be low. In addition, consumers get many benefits from mobile health apps in managing and quantifying their health and in finding support groups through peers. Therefore, the benefits derived from the usage of mobile health technologies might outweigh the privacy concerns they might have (Miller and Tucker, 2018, 2009; Tucker, 2014; Chellappa and Sin, 2005). In fact, the same Pew Research survey mentioned above found that about 41% of those surveyed find it acceptable to share their data with third parties. These mixed reactions could arise from the ubiquity of healthcare apps and the ambiguity in existing privacy policies. Therefore, it seems possible that an exogenous shock to female reproductive health could have no effect on mobile health and FemTech app usage.

However, it is also possible that consumers could actually increase the usage of health apps after the passage of the Dobbs ruling. For example, reproductive health-related issues change rapidly and constantly. Pregnancy and eligibility for abortions are time-sensitive issues — laws around abortion are built around "LMP" or the "last menstrual period", which might spur women to closely monitor their reproductive health and increase the usage of FemTech apps to track menstruation. In addition, media discussions on health apps in this period could increase awareness of the existence of these apps and increase their usage.

Finally, consumers could also reduce the usage of health and/or FemTech apps in re-

sponse. Before the passage of the Dobbs ruling, consumers might have been aware of the commercial surveillance of health app data – data being potentially used by third parties for targeted advertising. However, post-Dobbs, there was an unprecedented increase in awareness of how digital data, and digital health data in particular, could potentially allow the government to incriminate citizens (Torchinsky, 2022; Kim, 2022; Cox, 2022a; Collier and Burke, 2022; Edelson, 2022). Media reports pointed out the possibility that the digital histories of people seeking reproductive care could be analyzed for potential abortion in states where abortion was criminalized. Concerns about data privacy and government surveillance have been studied separately by privacy researchers (Buckman et al., 2023; Adjerid et al., 2016; Brandimarte et al., 2013; Goldfarb and Tucker, 2019). Roe v Wade being overruled meant that states would thereafter diverge much more sharply in their laws relating to abortion. That created, for the first time, a situation where state attorneys general in highly restrictive states could lawfully subpoena app or location information from firms located in states with looser abortion laws, and those firms would not necessarily have the ability to refuse a lawful subpoena for that information. Therefore, even women living in states with those looser laws, could not depend on firms in their states to protect women seeking reproductive healthcare, making the threat seem closer to home for a broader array of women. This could lead to chilling effects in their usage of digital services, and could manifest itself as a reduction in the usage of apps that track sensitive data.

To answer this question, we use a novel panel of mobile phone 'touch stream' data and an exogenous shock of publicity around health data privacy concerns. A draft of the Dobbs decision was leaked to the media on May 2, 2022.[4] The leak of the decision was a prior unknown, and hence we use the timing of the leak as an exogenous shock in our analysis. Our data provide us with detailed user-session-level usage with different apps and allow

[4] https://www.politico.com/news/2022/05/02/supreme-court-abortion-draft-opinion-00029473

us to estimate demand for these apps before and after the news about the Dobbs ruling became public. We use the timing of the Dobbs ruling becoming public as our exogenous shock in causally estimating the impact of potential government surveillance on the usage of health apps. We are the first to document whether and how an increase in tangible privacy concerns about government surveillance of digital data, particularly related to reproductive health, can lead to a change in the consumption of health apps and other privacy-preserving behaviors.

Our results reveal several interesting findings. First, we find that the number of sessions of health apps being used decreased by 9.6% compared to control apps in the aftermath of the Dobbs ruling. We also observed a 31% reduction in the average time spent on health apps, with a large decrease in the use of health apps among women. Specifically, women reduced the usage of health apps by 7.6% compared to men in terms of number of sessions and 26.7% in terms of the average time spent on apps. Second, we find that the usage of FemTech apps that track or provide information about women-specific issues decreased by 18.6% sessions and 66.7% in terms of the average amount of time among women.

Our findings indicate a significant and chilling effect among users of health apps. We explore several mechanisms that could contribute to this effect. We find that the chilling effect is higher among users who had a greater pre-treatment exposure to social media and news apps. This reveals that the chilling effect is higher among those who were already more aware of the increased publicization of governmental surveillance and how digital health data could be used by the government.

Our findings also demonstrate interesting ways in which users cope with the increased probability of governmental surveillance. Post-Dobbs, we see an increase in the usage of privacy-preserving technology apps such as DuckDuckGo, Brave Browser, Opera, etc. This increase is driven mainly by users who have never used these apps before the Dobbs ruling. This shows that the increase in privacy-preserving behavior is driven by users who suddenly

become aware of privacy concerns when their data could be used by the government.

This paper contributes to several strands of emerging literature on the social impacts of technology adoption. First, we contribute to the growing literature on the adoption of mobile health apps (Bardhan et al., 2020). Several studies in this literature have shown the impact of mobile health app adoption on health and how individuals have improved health outcomes, increased awareness, and improved their ability to self-manage health conditions. Our study shows how privacy concerns, particularly about digital health data and government surveillance, can discourage consumers from using these apps despite the important benefits they provide consumers. Several studies in the health informatics literature document inconsistent privacy policies even among apps that are used to track reproductive health (Shipp and Blasco, 2020; Aronson and Rehm, 2015). Second, our study also contributes to the literature on the privacy versus personalization debate. Personalization is one of the main reasons consumers adopt mobile health apps, as they can receive personalized recommendations to manage health concerns (Ghose et al., 2022). However, personalization and the adoption of AI also come at the cost of handling, storing, and even using sensitive consumer data. Although consumers may implicitly allow the usage of their data in exchange for personalized recommendations, it is unclear how these data might be shared with commercial entities and governmental agencies, especially since digital data is increasingly used in legal proceedings (Stuart, 2022). Our paper sheds light on how privacy concerns can interact with technology adoption using an exogenous shock to health privacy and thus, contributes to the literature on chilling effects.

Our work contributes to managerial and policy discussions on how to legislate and enforce policies around health apps. Our findings contribute to the highly litigated and increasingly prevalent issue of the admissibility and use of digital data in prosecutions (Nelson, 2024). In particular, since the landmark Carpenter ruling, which extended the Fourth Amendment rights to digital data, there have been different interpretations of what constitutes reasonable

expectations of privacy from a phone provider, what the exceptions are, and how digital data requests from technology firms pertain to the protections afforded by the Fourth Amendment. Our results show that when faced with the threat of surveillance, consumers reduce their participation in mobile health apps — an ecosystem where data privacy policies are ambiguous. Prior studies show how privacy-reducing and privacy-protecting regulations can impact public participation in public health programs (Buckman et al., 2023). We extend this literature to show how large changes in policies about women's health and the potential awareness of how digital data can be used by the government can influence consumers' participation in self-managing their health through technology, both men and women alike. FemTech apps have been shown to empower women with relevant information on their health. However, chilling effects arising from the government's use of health information could disincentivize technology adoption and usage.

# 2 Literature Review

We contribute to several streams of literature, as outlined below.

## 2.1 Mobile Health and FemTech Apps: Consumption, Benefits, and Interventions

Mobile health apps have been well-studied in the medical and healthcare IT literature. Extant studies have looked at the different aspects of health IT and how they can benefit physicians and patients alike (Bardhan and Thouin, 2013; Bardhan et al., 2020; Adler-Milstein et al., 2014). Recent studies show that the COVID-19 pandemic further spurred the virtualization of healthcare processes, with telehealth visits accounting for about a quarter of all healthcare visits, leading to a significant increase in access and a decrease in healthcare costs (Ayabakan et al., 2024; Bestsennyy et al., 2021). Mobile health apps play a key role in the

virtualization process of healthcare. In addition, the meteoric increase in smartphone adoption has led to the mass usage of wearable devices and the corresponding mobile health apps and platforms to collect data, support, track, and manage health conditions and compliance, and improve communication with patients (Estrin and Sim, 2010; Tomlinson et al., 2013; Heerden et al., 2012; Qiang et al., 2011). Investments in healthcare platforms (Bestsennyy et al., 2021), improvement in monitoring devices, sensors, and processors, coupled with the recent use of AI to collect and process large amounts of granular and real-time data, have all enabled this large-scale adoption (Agarwal et al., 2020; Brohman et al., 2020; Agarwal et al., 2023; Jiang and Cameron, 2020; Aramendi et al., 2018).

While the benefits of mobile health technologies have been well-documented, some studies in this literature have focused on devising strategies to improve the efficacy of healthcare management through these technologies and healthcare platforms that support these technologies (For a detailed review, see Lancaster et al. (2018) and Marcolino et al. (2018)). For example, Pop-Eleches et al. (2011) show how text reminders improve adherence to antiretroviral treatment among HIV patients. Mobile health apps and wearable devices also provide greater flexibility of use compared to browser-based technologies. This creates a large difference in how patients use these apps as patients don't have to log in at a physical PC station. Ghose et al. (2022) demonstrate how mobile health platforms show a 21.6% increase in patient health outcomes compared to PC versions of the same app.

There are special categories of apps designed for women to monitor their reproductive health more closely. These FemTech apps include a wide array of products — wearable devices such as patches, rings, bands, bracelets to mobile apps — that provide real-time data that closely monitor fluctuations in reproductive health throughout the menstrual cycle (Sohda et al., 2017). Studies find that women extensively use FemTech apps to monitor their reproductive health, including planning for pregnancy and/or contraceptives (Gambier-Ross et al., 2018), ovulation, premenstrual syndrome (Riley and Paskova, 2022), hormonal changes

(Mathiason, 2023), and menopause. Studies document how FemTech apps enable women to self-manage changes in their body and behavior, be aware of their body, and have informed conversations with their physicians (Epstein et al., 2017). FemTech apps have seen large-scale adoption in the last few years, with industry reports estimating the presence of 1500 FemTech firms and $22.83 billion worth of investment in this area just in 2023.[5]

Although the importance and benefits of mobile health and FemTech apps have been documented, concerns surrounding their usage have not been studied in detail. Most of the studies in the IS literature have addressed different strategies that firms could adopt to engage users on these apps. In our study, we focus on the reasons that could prevent consumers from using these apps despite the benefits consumers derive from personalization, which reveals significant privacy concerns following the threat of government surveillance.

## 2.2 Privacy Vs. Personalization

The increase in demand for mobile health apps, combined with a low barrier to entry, has also led to the proliferation of these apps in the market. Studies in this literature evaluate mobile health apps according to different parameters and find that users of health and fitness apps have several privacy and safety concerns about how these apps handle their health data (Hutton et al., 2018; Scott et al., 2015). Despite the sensitive nature of the data collected by mobile health apps, there are few frameworks to govern mobile health apps around the world. Within the U.S, the Food and Drug Administration (FDA) regulates only apps and software that are part of medical devices.[6] Despite policymakers' attempts to provide guidance to govern mobile health apps, regulation of the large mobile health market has proven to be difficult; the apps on the market vary greatly in quality and security (Larson, 2018; Sheppard, 2020).

[5] https://pitchbook.com/blog/what-is-femtech

[6] https://www.fda.gov/medical-devices/digital-health-center-excellence/device-software-functions-including-mobile-medical-applications

In addition to security, there is a significant gray area in how privacy is enforced in these apps. Each firm determines its privacy policies for mobile health apps, and each firm decides how to handle the large trove of sensitive health data collected from customers in accordance with its own policies. Shipp and Blasco (2020) evaluate the privacy policies of top FemTech apps and find that the language conveying privacy policies was ambiguous, with the language indicating that the reproductive data were shared with third parties. Responsible collection, storage, and processing of healthcare data are paramount in realizing the benefits of personalization in healthcare (Aronson and Rehm, 2015). This is even more salient in the context of data that could be misused by employers or insurers, particularly among vulnerable populations (Miller and Tucker, 2018).

Interestingly, personalization plays an important role in the adoption of mobile health apps. Studies show how AI-based personalization can significantly transform the healthcare system (Johnson et al., 2021; Mehta et al., 2020; Zhang et al., 2018). For example, wearable devices, mobile health apps, and personalization within these apps can improve self-management of health conditions and patient outcomes for chronic health conditions like diabetes and asthma (Reddy et al., 2016). Fitness trackers have also shown to be particularly effective in influencing positive changes in behavior and clinical outcomes through personalization and gamification, thus improving adherence and compliance to clinical recommendations (Rowland et al., 2020; Perski et al., 2017). The value of personalization in healthcare creates an interesting privacy vs. personalization paradox, which has been studied in the healthcare and privacy literature (Miller and Tucker, 2009; Goldfarb and Tucker, 2011). Consumers who find significant utility from personalization might also be concerned about the risks of the ambiguity of how personalization algorithms process their data, which can significantly reduce the adoption and use of technology (Lee and Gostin, 2009; Miller and Tucker, 2018). While prior studies in the literature have focused on privacy concerns arising from the commercial use of data (Tucker, 2014), this research focuses on how aware-

ness of potential prosecution by the government on matters of reproductive health can affect the diffusion of technology, especially among the population that will benefit from such technology.

## 2.3 Chilling Effects

Much of the literature on health privacy regulation and the impact of technology diffusion has analyzed data privacy from the perspective of competition and commercialization of consumer data. More specifically, the debate in this literature has focused on the commercial nature of privacy, how firms can potentially leverage information about consumers, and whether regulations can affect the nature of competition. The other important dimension of this discussion is about the role of governments and why citizens might want to protect personal information from the government.

More specifically, fear of state surveillance might lead consumers to significantly alter their behavior on the Internet, leading to chilling effects (Penney, 2017). According to legal scholars, chilling effects are a consequence of mistrust and uncertainty in the laws and legal systems of a country that citizens self-censor themselves in engaging even in regular and legal activities (Schauer, 1978; Penney, 2017). The idea of government surveillance of Internet activities came into prominence after the Snowden revelations, which were a highly visible exogenous shock to people's perception of privacy (Marthews and Tucker, 2017; Penney, 2017). In fact, a Pew Research survey, two years after the Snowden revelations, found that 9 out of 10 people had heard about government surveillance programs, and at least 41% of those surveyed had changed at least one of their behaviors.

The Dobbs ruling provides us with an exogenous shock to study chilling effects in the context of the healthcare industry. In particular, the Dobbs ruling brought out inconsistencies in the ambiguities in how app or location information could be lawfully accessed by the government in states with strict abortion laws, even if the technology firm was lo-

cated in states with looser abortion laws. This divergence in laws relating to reproductive health made the idea of government surveillance much more salient nationally and could, paradoxically, produce chilling effects even if the need for mobile health apps could increase. This brings us to the theoretical framework, where we develop a series of hypotheses to test whether exogenous shocks about privacy related to health would lead to a chilling effect in the use of health apps.

# 3 Development of Hypotheses

## 3.1 Chilling Effects

The reactions to censorship and surveillance have been studied in the psychology literature. In fact, Jack and Sharon Brehm's seminal work on psychological reactance (Brehm, 1966; Brehm and Brehm, 2013) provides us with a deep insight into how people might react when their freedom is under threat and what factors might moderate this effect. This theory states that people will react to restore their subjective perception of freedom when their freedom is restricted. Further, reactance to freedom is not based on whether there is an actual threat, but rather on the perception of a threat to freedom. The stages of psychological reactance might inform us about the possible outcomes in the context of Dobbs ruling as outlined below.

Brehm and Brehm (2013) argue that for a person to react to the elimination of freedom to do something, the person should know about the existence of that specific freedom, even if the person does not exercise the freedom. In the context of reproductive rights, abortions have been legal in the United States since the passage of Roe v. Wade in 1973. While abortions have been a controversial topic in political, social, religious, and legal discourses, most people in the United States are aware of the ability to get abortions regardless of whether they choose to exercise this freedom.

A ban or threat to a well-known freedom can trigger psychological reactance. The magnitude of reactance is influenced by various factors, such as the source of the threat and the frequency with which a person interacts with it. The third stage of reactance stems from the person's desire to restore their freedom. Depending on intensity, awareness, and competence, there can be a variety of responses to threats.

The Dobbs ruling enabled the passage of restrictive laws around abortion in some states, and it represented a large social and political shift in reproductive rights. The Dobbs ruling opened up a situation in which digital records from technology firms located in states with less stringent abortion laws could be subpoenaed by states with restrictive abortion laws to prove an impending pregnancy. Stuart (2022) documents an increasing number of requests for digital data in litigation. In other words, while the ruling itself was about abortion, the threat was that the government could surveil digital health data if the need arises.

The fourth stage of reactance is when a person engages in activities to attempt to restore the perceived loss of freedom. In the context of digital records, this can manifest itself as chilling effects, where people stop engaging in certain online activities to protect themselves from perceived threat. In fact, a flurry of news articles immediately after the Dobbs ruling described anecdotal evidence of how digital records were indeed used to ascertain information about an individual's reproductive health (Shipp and Blasco, 2020; Baker-White and Emerson, 2022; McQuillan, 2022; Zakrzewski et al., 2022; Stopczynski, 2015; Gross, 2024; Wright and Vazquez, 2022; Hill, 2022; Conti-Cook, 2020; Murphy, 2022; Joh, 2022; Carr Smyth, 2023). The articles advised readers to be aware of their digital footprint and offered suggestions on how to avoid tracking.

This opens up an interesting tension in our context. On the one hand, the idea of government surveillance might not be new to individuals. Individuals might have always perceived digital records to be vulnerable to government surveillance, especially since prior high-profile incidents such as the Snowden revelations might have brought it to their attention. In this

case, we would not expect any changes in the way people use mobile health apps. On the other hand, a sudden increase in awareness of a highly politicized and publicized threat to reproductive rights, unclear laws on how technology-firms will handle subpoenas from states where they are not located, and tangible repercussions of the use of a person's digital records might create a strong reactance in the form of chilling effects. In addition, awareness of the privacy repercussions of the Dobbs ruling was made even more salient due to the unprecedented number of political advertisements run throughout the United States, and not just in the states that passed restrictive laws around abortions immediately after the Dobbs ruling.[7] Interestingly, the locus of threat has been explained by scholars who study reactance theory. Andreoli et al. (1974) posit that the reactance to the threat of previously available freedom is salient even among people who do not experience a threat to their freedom but are made aware of others who experience the threat. Andreoli et al. (1974) explain that this could be due to the anticipated loss of their own freedom.

In our context, even if the articles about the Dobbs ruling were focused on women's reproductive choices, they might have created a large-scale awareness of how digital health data could be used by anyone outside the realm of commercial interest. In fact, studies show that the reactance is relatively higher when the perceived threat to freedom is the government compared to other agents (Ng et al., 2021). This brings us to our hypotheses H1a and H1b.

If the government's use of digital health data is the perceived threat, the reactance to this perceived threat should be highest for the data that is considered to be the riskiest in the context of the threat among the population the most vulnerable to the perception of threat. More specifically, if people are made aware of the potential use of reproductive health-related data, we should observe the highest reactance among apps that track female reproductive health. This gives us our H1c.

[7] https://www.politico.com/news/2022/12/19/dobbs-2022-election-abortion-00074426

**Hypothesis 1** ***Hypothesis 1a*** *Usage of mobile health apps decreases after the Dobbs ruling*

***Hypothesis 1b*** *The reduction in usage of mobile health apps after the Dobbs ruling is higher among women than men*

***Hypothesis 1c*** *Usage of FemTech apps decreases after the Dobbs ruling.*

## 3.2 Awareness

As reactance theory shows, there can be several moderators of how people could react to the threat of their privacy. To begin with, reactance could be a function of awareness. Unlike the Snowden revelations, digital privacy was not the direct subject of the Dobbs ruling. In the Dobbs ruling, most of the news coverage was about reproductive rights, access to abortions, and how this would vary between states. Conversations about digital privacy were a consequence of the passage of restrictive abortion laws in some states, even if technology firms were located in states with less stringent abortion laws. Therefore, awareness of the privacy implications of the Dobbs ruling would be a function of higher news consumption.

Following the leak of the Dobbs ruling, social media platforms such as Facebook, Twitter, and Tiktok were filled with users taking a stance on this divisive issue, sharing experiences and anecdotes and showing their support for causes (Pleasure et al., 2024).[8,9] Thus, people who are more aware of the real-life consequences of laws affecting digital privacy could be more likely to reduce their digital footprint.

There is a large body of literature that surrounds the production, distribution, and consumption of misinformation and less credible news on the Internet. Rumors and misinformation about mass surveillance are among the topics that are the most talked about in

[8] https://apnews.com/article/abortion-health-dallas-government-and-politics-business-e6fbd819541a3fda6930b292e2f91a9e

[9] https://www.businessinsider.com/olivia-julianna-abortion-fundraiser-trolled-matt-gaetz-2-million-dollars-2022-8

online forums and misinformation sites (Samory and Mitra, 2018). If there is prior exposure to misinformation and general mistrust of the government, repeated exposure to the possibility of greater surveillance by the state of reproductive healthcare could induce higher chilling effects. In fact, Pennycook and Rand (2021) examine the psychology of misinformation and find a positive association between accepting claims (reflexive open-mindedness) and the tendency to believe in low-credibility information. Studies in this literature find a positive association between familiarity, repeated exposure, and an increase in perceptions of accuracy, even if the information is not credible (Pennycook et al., 2018; Fazio et al., 2015). In other words, even if the actual number of subpoenas from the government might not be high, people who consume higher levels of low-quality news might be prone to more distrust of the government and big-tech firms and might change their behavior on mobile health apps.

This brings us to our next set of hypotheses H2a, H2b and, H2c on the role that awareness plays in moderating the usage of mobile health apps.

**Hypothesis 2** ***Hypothesis 2a*** *The decrease in the usage of mobile health apps after the Dobbs ruling is higher among users with higher pre-treatment usage of social media.*

***Hypothesis 2b*** *The decrease in the usage of mobile health apps after the Dobbs ruling is higher among users with higher pre-treatment news consumption.*

***Hypothesis 2c*** *The increase in chilling effects is higher among users with higher visits to low-credibility websites.*

## 3.3 Demographics

Research has shown that individual demographic characteristics such as race, age, and income can have a significant impact on privacy concerns (Zukowski and Brown, 2007). Research

on the moderating effect of race and ethnicity on people's privacy outlook has shown mixed results. Li et al. (2021); Frik et al. (2022) suggest that race and ethnicity do not significantly impact people's privacy concerns. However, Ghose et al. (2020) shows that cities with larger white populations were more concerned with privacy during the COVID-19 pandemic, suggesting that there could be a demographic component to privacy, particularly in the context of digital health-related data. In addition, it is entirely possible that age might influence privacy concerns surrounding digital data. Younger consumers of childbearing age might be more aware of the news about reproductive health post-Dobbs, which, in turn, might decrease the usage of mobile health apps. Moreover, younger users are more aware of privacy concerns (Blank et al., 2014), particularly in digital settings such as using social media sites (Bergström, 2015).

In addition to race, income might play an important role in moderating the usage of mobile health apps. Historically, low-income communities have shown increased privacy concerns with digital surveillance (Madden et al., 2017). They are disproportionately targeted with predatory products like payday loans and other financially unsafe products (Gilman, 2020; O'neil, 2017), and also by government surveillance (Buckman et al., 2023). For example, there have been reports that law enforcement-managed cameras equipped with facial recognition are more likely to be deployed in low-income communities (Ferguson, 2017). Interestingly, Anderson et al. (2024) show that following the Dobbs ruling, income is an important moderator of mental health in the context of reproductive health. Therefore, low-income groups are generally likely to have greater privacy concerns about their personal data being used by government agencies, which might lead to a larger impact of the Dobbs verdict on mobile health app usage. The role of demographics in chilling effects is our focus in the next set of hypotheses.

**Hypothesis 3** ***Hypothesis 3a*** *Usage of mobile health apps after the Dobbs ruling decreases more among white users.*

***Hypothesis 3b*** *Usage of mobile health apps after the Dobbs ruling decreases more among younger users.*

***Hypothesis 3c*** *Usage of mobile health apps after the Dobbs ruling decreases more among low-income users.*

### 3.4 Privacy-Preserving Behaviors

Reactance theory hypothesizes that a threat to freedom can trigger an individual to restore that freedom (Brehm and Brehm, 2013). In our context, if users are threatened by the government's access to sensitive data, they should be finding ways to preserve their digital privacy. This has been demonstrated through customer surveys (Potoglou et al., 2017) and increased traffic to privacy-preserving search engines after the Snowden revelations (Rosso et al., 2020). Therefore, it is likely that we would observe an increase in the usage of privacy-protecting browsers post-Dobbs. In addition, the increase in usage is likely driven by users who have not adopted these browsers prior to the passage of the Dobbs ruling.

**Hypothesis 4** ***Hypothesis 4a*** *Use of privacy-preserving browsers after the Dobbs ruling increases*

***Hypothesis 4b*** *The increase in the use of privacy-preserving browsers is driven by new users (those who did not use these browsers pre-Dobbs).*

## 4 Data

### 4.1 Mobile Usage Panel

Our primary data source consists of detailed smartphone usage obtained by a US-based market intelligence firm. The data consists of a population representative panel of opt-in

Android users in the United States. The usage data was collected via a smartphone app in a fully GDPR/CCPA compliant manner, and the users were paid a fixed fee for each month they had the app installed on their phones. For each user in the panel, we observe anonymized real-time smartphone usage activity. To ensure rectangularization of the panel, we include only those users who entered the panel four weeks before the Dobbs verdict leak and exit the panel six weeks after the leak — this exercise leaves us with a panel of 1322 users. Every time a panelist uses their smartphone, we observe the app being activated in the foreground, along with a timestamp of the activity. Each entry is also associated with a unique session identifier. Given that most smartphone activity is carried out on individual apps, our data allows us to extract granular insights into the overall smartphone usage of our panelists.

However, since we are unable to identify the activity performed within each app, our data do not allow us to identify the actions being performed within these apps. Nevertheless, we can still make significant observations based only on the applications that are used.

**App-Classifications data**: The data provider had pre-classified the apps based on their Google Play Store category. Since our primary goal is to analyze the impact of the Dobbs ruling on specific app usage, we use all the apps in our analysis that fall under the health and fitness category. Further, we manually curate the list to exclude insurance and pharmacy apps.

In addition, health and fitness apps have different subcategories. While each app tends to focus on specific functions such as step tracking, diet tracking, and running, many have additional health-related features. For example, most fitness or step tracking apps also have features to track diet and menstrual cycles to provide a holistic approach to monitoring health.

We also classify applications that provide features to track women's reproductive health as "FemTech" apps. We obtained a large list of such apps using keywords such as "period",

"mensuration", "ovulation", "fertility", "pregnancy" in the app names and descriptions of the apps in the Google Play store.

We also have detailed self-reported demographic data like gender, age, race, and median annual household income for the users in our panel. To identify the heterogeneous impact of age, we use the median split of users' age to classify them as younger (less than or equal to 45 years) and older (more than 45 years) users. Similarly, for income, we split the users into low-income (less than $50,000 per year) and high-income (more than or equal to $50,000 per year) groups. For race-related heterogeneity, we classify the user into white and non-white depending on their self-reported race details. Users without demographic information are omitted from the heterogeneity analyses.

Table 1 shows the split of users in our sample according to different demographic characteristics.

Table 1: Sample Size by Demographic Characteristics

| | N |
|---|---|
| **Gender** | |
| Female | 928 |
| Male | 392 |
| **Age** | |
| Young | 655 |
| Old | 667 |
| **Race** | |
| White | 836 |
| Non-White | 364 |
| **Income** | |
| Low-Income | 527 |
| High-Income | 714 |

**Website Visits**:

Our data provider also provides us with the website visit logs of all users through their smartphone browser apps. The data identifies all the link clicks and redirects that happen

from other apps on a user's phone. More specifically, even though we do not observe what users are specifically interested in a webpage, we know all the URLs (Uniform Resource Locator) they visit. Since URLs can be very specific, we extract the domain-level information from the URLs and use these domains in our analyses. Our domain-level webpage visit data allows us to identify different types of webpages, like news websites, that our users visit.

**MBFC**:

To identify exposure to political bias and misinformation in websites visited by our panelists, we use data from Media Bias Fact Check (MBFC), an independent platform that keeps track of bias and minsinformation ratings of about 8,200 news websites in the United States.[10] By matching the website domains in our data with news websites, we can exactly identify the exposure of each user in our panel to politically biased media as well as misinformation.

**Privacy Preserving Browsers**

Digital marketers collect private information such as browser cookies, IP addresses, and device-specific identifiers via websites visited by users. This information is then sold to advertisers in exchange for a monetary gain which helps advertisers target the users with specific product recommendations. However, in recent times, there have been growing privacy concerns over the user data collected in such a manner, and several web browser based apps have started restricting websites from collecting such information. Users who are particularly concerned about their digital privacy use these browser apps for their web-related activities. To test for such a shift as the result of the Dobbs verdict in our data, we check the usage of three popular privacy-preserving browser apps - Brave, DuckDuckGo, and Tor Browser (Radivojevic et al., 2024).

[10] `https://mediabiasfactcheck.com/`

# 5 Empirical Analysis

## 5.1 Context

The legal status of abortion has been part of an intense debate throughout the history of the United States. Up until 1973, the legal status of abortion was decided by individual states. In the landmark *Roe v. Wade* case, the United States Supreme Court granted legal protections to abortion rights on January 22, 1973. The verdict struck down existing abortion laws and provided protection against prosecution for those seeking an abortion.

On June 24, 2022, following up on a challenge by the state of Mississippi, the U.S. Supreme Court struck down the protections offered by *Roe v. Wade* under the *Dobbs v. Jackson* verdict. However, a draft of the decision was leaked to the media on May 2, 2022,[11] much earlier than the anticipated date of the verdict. Given that the leak of the decision, as well as the final verdict, had been *a priori* unknown, the event presents an exogenous shock to identify the impact of the verdict on privacy-motivated digital behavioral changes.

Concerns about the usage of digital traces in abortion-related prosecutions have been ongoing for almost a decade. For example, the use of smartphone search history and text messages in such cases (Zakrzewski et al., 2022; Stopczynski, 2015; Gilman, 2021) has been covered in depth by national and local media channels. After the Dobbs verdict leaked, concerns about law enforcement agencies using digital data in abortion-related prosecutions gained a lot of media attention (Carr Smyth, 2023). News outlets highlighted how digital data - such as text messages, personal chats, search queries, app usage metrics, and GPS location history of smartphones, could be used to convict people who reside in states with strict limits on abortion (Baker-White and Emerson, 2022; Cox, 2022b).

As a result of such concerns, calls to either completely delete period tracking apps or

[11] https://www.politico.com/news/2022/05/02/supreme-court-abortion-draft-opinion-00029473

reduce the usage of such apps gained traction in media outlets and on social media platforms (Trau, 2022; McQuillan, 2022). This also led legal scholars to document and comment on the increasing cases of the use of digital data in abortion-related prosecutions (Nelson, 2024; Stuart, 2022; Conti-Cook, 2020). Importantly, this ruling came at a time when electronic records were increasingly used in legal proceedings. Legal scholars document how information from fitness trackers is now a regular part of legal proceedings and litigation (Stuart, 2022; Jr, 2017; Righney, 2019). Following the media leak of the Dobbs ruling, technology platforms made several platform-level changes and reiterated their commitments toward protecting users' data; however, concerns regarding safety remained significant (Walter and Tsang, 2022; Thibault, 2022; Fitzpatrick, 2022; Cox, 2022c; Hill, 2022).

In addition to media attention over privacy concerns, Anderson et al. (2024) also show increased mental distress after the Dobbs verdict, highlighting the importance of the decision to US residents in general. In summary, when the Dobbs verdict was leaked, there was heightened concern, particularly over state and local government agencies subpoenaing digital data to aid in prosecution. Despite assurances from technology platforms, users were concerned about the privacy implications of their digital data being collected and used by the government.

The media leak of the Dobbs ruling generated a lot of interest and the potential implications of that ruling were covered in several news articles from major news outlets.[12,13] In fact, much of the news articles written about the implications for digital privacy were written before the actual ruling. Thus, we treat the advance leak of the ruling as the exogenous event, instead of the actual verdict date.

[12] https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps

[13] https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/

## 5.2 Model

Using the same set of users of mobile health applications that we observe in our data for the entire analysis window, we construct a balanced panel at the user-app-week level and estimate the following DiD model:

$$y_{ijt} = \beta_1 Post_t + \beta_2 mHealth_j + \beta_3 Post_t \times mHealth_j + \alpha_i + \gamma_j + \tau_t + \epsilon_{ijt} \quad (1)$$

where $i$ refers to the user, $j$ refers to the app, $t$ refers to the week in the data. The outcome variables are the total number of sessions and the total time spent using each app $j$ by each user $i$ in each week $t$.

$Post_t$ is the event variable that takes a value of 1 if the week $t$ follows the first week after the Dobbs ruling was leaked on Politico (May 2, 2022). $mHealth_j$ takes the value 1 if app $j$ is a mobile health app, and 0 for the control app. In our analysis, we used Pinterest as our control app, since the discussions about Roe v. Wade were very high on other social media apps. Pinterest differs significantly from other social media platforms, as the content shared on Pinterest is predominantly image-based and dominated by women (Ottoni et al., 2013). Further, unlike Instagram, TikTok, and Facebook, where the focus is on content creation, the focus on Pinterest is image curation, like a virtual scrapbook (Mittal et al., 2013; Kasakowskij et al., 2020). We also use other apps, such as games, as controls in our robustness checks and find consistent results. $\alpha_i$, $\gamma_j$, and $\tau_t$ are fixed effects for user, app, and week, respectively. In this model, the coefficients corresponding to $Post_t$ & $mHealth_j$ are dropped because they are collinear with the user, app, and time-fixed effects. We use a time window of 4 weeks prior to and 6 weeks after the Dobbs ruling leak. The standard errors are clustered at the user level.

## 5.3 Results - Chilling Effects After Dobbs

We present the results from estimating Equation 1 in Table 5. The results suggest that, overall, the usage of mobile health apps decreased by 9.6% (1 - exp(0.092)) during the 6 week period following the leak of the Dobbs ruling compared to the usage of the control app. Moreover, we see a decrease in mobile health app usage among both women and men, although women reduce usage much more than men (12.1% as opposed to 4.2% reduction by men.) Table 6 estimates Equation 1 using total weekly time an app was used by each user instead of the number of sessions as the variable of interest. Our results show that the Dobbs leak's impact is consistent across different measures of mobile app usage. We find the chilling effects even starker in the app usage time. More specifically, we find a 31% drop in usage among all users. Further, we see a 26.7% greater drop in mobile health app usage among women compared to men. These results point towards a chilling effect inhibiting people's usage of mobile health apps following the Dobbs ruling, confirming hypotheses 1a & 1b.

In column (5), we check the usage of FemTech apps instead of mobile health apps relative to the usage of the control app after the Dobbs verdict leak. Our results show an 18.6% decrease — much larger than the impact on usage of mobile health apps. Finally, we also see a stark 66.7% drop in time use of FemTech apps following the Dobbs ruling, confirming hypothesis 1c.

## 5.4 Event Study

We verify the parallel trends assumption using the following event study specification.

$$y_{ijt} = \alpha_i + \gamma_j + \tau_t + \sum_{w=-4}^{w=6} \beta_w * 1[t = w] * mHealth_j + \epsilon_{ijt} \tag{2}$$

Table 2: Impact of Dobbs on Usage of Mobile Health Apps (Sesisons)

| Dependent Variable: | Log(Sessions) | | | |
|---|---|---|---|---|
| | All Users | Female Users | Male Users | FemTech Apps |
| | (1) | (2) | (3) | (4) |
| *Variables* | | | | |
| Post × mHealth App | -0.092*** | -0.114*** | -0.041** | -0.171*** |
| | (0.011) | (0.014) | (0.016) | (0.021) |
| User Fixed Effect | Yes | Yes | Yes | Yes |
| App Fixed Effect | Yes | Yes | Yes | Yes |
| Week Fixed Effect | Yes | Yes | Yes | Yes |
| $R^2$ | 0.02604 | 0.03071 | 0.01955 | 0.10192 |
| Observations | 9,481,384 | 6,655,616 | 2,811,424 | 219,615 |

The indicator variable $1[t = w]$ takes a value of 1 if the calendar week $t$ is $w$ weeks apart from the week of the Dobbs verdict leak. The baseline period is -1, which means that the average change in the usage of mobile health apps compared to the usage of the control app is measured relative to the difference in the usage one week before the Dobbs leak.

Figure 1 shows the estimates from Equation 2 along with the 95% confidence intervals. We see that before treatment, there was no significant difference in the use of mobile health apps relative to the control app. This verifies the parallel trends assumption (Autor, 2003; Agarwal and Sen, 2022; Greenwood and Agarwal, 2016). However, post-treatment, the usage of mobile health apps declined significantly compared to that of the control app.

To verify that our results are not influenced by the choice of control group app, we estimate Equation 1 using an alternate group of control apps. Specifically, we use some of the popular gaming apps on the Google Play Store platform - *Solitaire Grand Harvest, Clash Royale, Clash of Clans, and Candy Crush Saga.* Results presented in Table 7 show that our results are robust to the choice of the control group of apps.

Figure 2 confirms that the parallel trend assumptions are valid for the alternate control

Table 3: Impact of Dobbs on Usage of Mobile Health Apps (Time)

| Dependent Variable: | Log(Time) | | | |
|---|---|---|---|---|
| | All Users | Female Users | Male Users | FemTech Apps |
| | (1) | (2) | (3) | (4) |
| *Variables* | | | | |
| Post × mHealth App | -0.270*** | -0.341*** | -0.104** | -0.511*** |
| | (0.035) | (0.045) | (0.049) | (0.068) |
| User Fixed Effect | Yes | Yes | Yes | Yes |
| App Fixed Effect | Yes | Yes | Yes | Yes |
| Week Fixed Effect | Yes | Yes | Yes | Yes |
| $R^2$ | 0.02963 | 0.03588 | 0.02035 | 0.11545 |
| Observations | 9,481,384 | 6,655,616 | 2,811,424 | 219,615 |

group as well.

# 6 Mechanisms

## 6.1 Awareness

We now explore how the impact of the Dobbs ruling leak differed between different subgroups of users. First, we look at how social media usage moderates privacy concerns associated with using mobile health apps. We categorize our sample set of users into high versus low social media users based on the median split of the proportion of social media app sessions[14] relative to the total number of app sessions in a given week, during the four-week window before the Dobbs ruling leak.

Next, we look at how news consumption moderates the impact of the Dobbs ruling leak on the usage of mobile health apps. We use website visits data to identify all domain names belonging to news websites. We then calculate the fraction of visits to these domains relative

[14]We use all apps categorized by our data provider as Social Media apps.

Table 4: Impact of Dobbs on Usage of Mobile Health Apps - Alternate Control

| Dependent Variable: | Log(Sessions) | | |
|---|---|---|---|
| | All Users | Female Users | Male Users |
| | (1) | (2) | (3) |
| *Variables* | | | |
| Post × mHealth App | -0.019*** | -0.022*** | -0.011** |
| | (0.003) | (0.004) | (0.005) |
| User Fixed Effect | Yes | Yes | Yes |
| App Fixed Effect | Yes | Yes | Yes |
| Week Fixed Effect | Yes | Yes | Yes |
| $R^2$ | 0.01825 | 0.01969 | 0.01736 |
| Observations | 9,517,805 | 6,592,575 | 2,910,820 |

to the total number of website visits each week during the pre-period window. We split the users into high- and low-news-consumption users based on the median split of weekly fraction of news-consumption.

Finally, we check visits to all the domains listed in the MBFC list of websites to identify exposure to low-credibility news websites. We use the weekly fraction of visits to non-high credibility websites as identified by MBFC relative to visits to all the websites from the MBFC list, to identify users who were exposed to websites with low credibility news articles during the pre-period.

For each of the above conditions, we re-run the regression specification from Equation 1 using only the subsample of users relevant to that particular condition. The results are shown in Table 8.

From columns (1) and (2), we see that users with high pre-period social media usage had a larger drop in usage of mobile health apps compared to users with low social media usage, lending support to hypothesis 2a. Similarly, from columns (3) and (4), we observe that users with high pre-period news consumption had a larger drop in the usage of mobile health apps

Table 5: Impact of Dobbs on Usage of Mobile Health Apps (Sesisons)

| Dependent Variable: | Log(Sessions) | | | | |
|---|---|---|---|---|---|
| | All Users (1) | Female Users (2) | Male Users (3) | Triple DiD (4) | FemTech Apps (5) |
| *Variables* | | | | | |
| Post × mHealth App | -0.092*** | -0.114*** | -0.041** | -0.041** | -0.171*** |
| | (0.011) | (0.014) | (0.016) | (0.016) | (0.021) |
| Post × Female | | | | 0.073*** | |
| | | | | (0.021) | |
| mHealth App × Female | | | | -0.061*** | |
| | | | | (0.017) | |
| Post × mHealth App × Female | | | | -0.073*** | |
| | | | | (0.021) | |
| User Fixed Effect | Yes | Yes | Yes | Yes | Yes |
| App Fixed Effect | Yes | Yes | Yes | Yes | Yes |
| Week Fixed Effect | Yes | Yes | Yes | Yes | Yes |
| $R^2$ | 0.02604 | 0.03071 | 0.01955 | 0.02731 | 0.10192 |
| Observations | 9,481,384 | 6,655,616 | 2,811,424 | 9,467,040 | 219,615 |

Note: Robust standard errors clustered at user level in parentheses. The unit of observation is user-app-week. The dependent variable is log numer of sessions. Post is an indicator variable which denotes if the time period is after the Dobbs verdict was leaked. mHealth App indicates whether the app is a mobile health app or a control app.
$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.

compared to users with low pre-period news consumption, thus validating the hypothesis 2b. Together, these results suggest that increased exposure to potential privacy-related consequences is associated with higher chilling effects.

Columns (5) and (6) show that users with higher exposure to low-credibility news reduced the usage of mobile health apps much more than users with lower exposure to low-credibility news — in line with hypothesis 2c.

Table 6: Impact of Dobbs on Usage of Mobile Health Apps (Time)

| Dependent Variable: | Log(Time) | | | | |
|---|---|---|---|---|---|
| | All Users | Female Users | Male Users | Triple DiD | FemTech Apps |
| | (1) | (2) | (3) | (4) | (5) |
| *Variables* | | | | | |
| Post × mHealth App | -0.270*** | -0.341*** | -0.104** | -0.104** | -0.511*** |
| | (0.035) | (0.045) | (0.049) | (0.049) | (0.068) |
| Post × Female | | | | 0.238*** | |
| | | | | (0.067) | |
| mHealth App × Female | | | | -0.229*** | |
| | | | | (0.063) | |
| Post × mHealth App × Female | | | | -0.237*** | |
| | | | | (0.067) | |
| User Fixed Effect | Yes | Yes | Yes | Yes | Yes |
| App Fixed Effect | Yes | Yes | Yes | Yes | Yes |
| Week Fixed Effect | Yes | Yes | Yes | Yes | Yes |
| $R^2$ | 0.02963 | 0.03588 | 0.02035 | 0.03128 | 0.11545 |
| Observations | 9,481,384 | 6,655,616 | 2,811,424 | 9,467,040 | 219,615 |

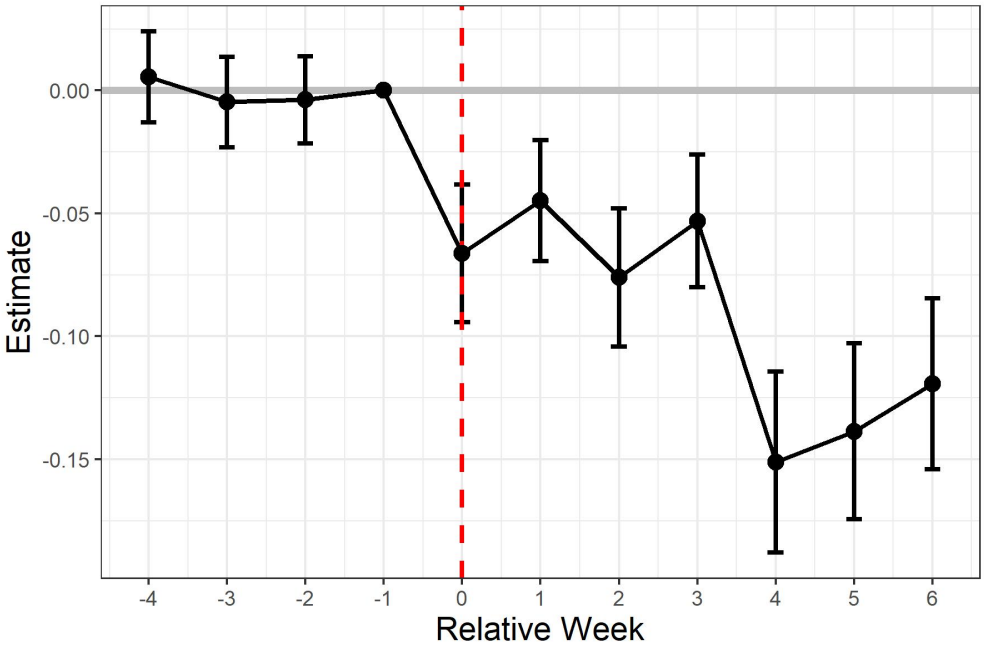
Note: Robust standard errors clustered at user level in parentheses. The unit of observation is user-app-week. The dependent variable is log total time. Post is an indicator variable which denotes if the time period is after the Dobbs verdict was leaked. mHealth App indicates whether the app is a mobile health app or a control app.
$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.

## 6.2 Demographics

Table 9 shows how the impact of the Dobbs decision varied by users' demographic characteristics. We use three different self-reported demographic characters of our panel of users - race, age, and median annual household income. Columns (1) and (2) compare the impact across white and non-white users. Our results suggest that white users are more privacy conscious than non-white users — we find that white users decreased the use of mobile health apps much more than non-white users, which confirms hypothesis 3a.

In columns (3) and (4), we use the median split of users' age to compare the impact

Figure 1: Event Study Estimates




Note: The figure shows event study estimates of mobile health app usage relative to Pinterest usage. The dependent variable is the log number of weekly sessions. The unit of observation is at the user-app-week level. 95% confidence intervals are shown.

between younger and older users. In line with our hypothesis 3b, we find that younger users reduce the use of fitness tracking apps more compared to older users. This could occur for two reasons. Younger users are likely to be more technologically savvy (Blank et al., 2014) and are aware of privacy concerns. Further, younger users of childbearing age are more likely to be aware of the news about the privacy concerns around reproductive health.

Finally, in columns (5) and (6), we divide the users by median annual household income to compare the impact across income levels. Our results suggest that income is an important factor in self-censoring. Anderson et al. (2024) show how the Dobbs ruling impacted mental health among low-income groups. Following this, we find that low-income users were particularly more likely to reduce the use of health apps compared to control apps after the Dobbs confirming hypothesis 3c.

Table 7: Impact of Dobbs on Usage of Mobile Health Apps - Alternate Control

| Dependent Variable: | Log(Sessions) | | | |
|---|---|---|---|---|
| | All Users | Female Users | Male Users | Triple DiD |
| | (1) | (2) | (3) | (4) |
| *Variables* | | | | |
| Post × mHealth App | -0.019*** | -0.022*** | -0.011** | -0.011** |
| | (0.003) | (0.004) | (0.005) | (0.005) |
| Post × Female | | | | 0.011* |
| | | | | (0.006) |
| mHealth App × Female | | | | 0.007 |
| | | | | (0.007) |
| Post × mHealth App × Female | | | | -0.011* |
| | | | | (0.006) |
| User Fixed Effect | Yes | Yes | Yes | Yes |
| App Fixed Effect | Yes | Yes | Yes | Yes |
| Week Fixed Effect | Yes | Yes | Yes | Yes |
| $R^2$ | 0.01825 | 0.01969 | 0.01736 | 0.01828 |
| Observations | 9,517,805 | 6,592,575 | 2,910,820 | 9,503,395 |

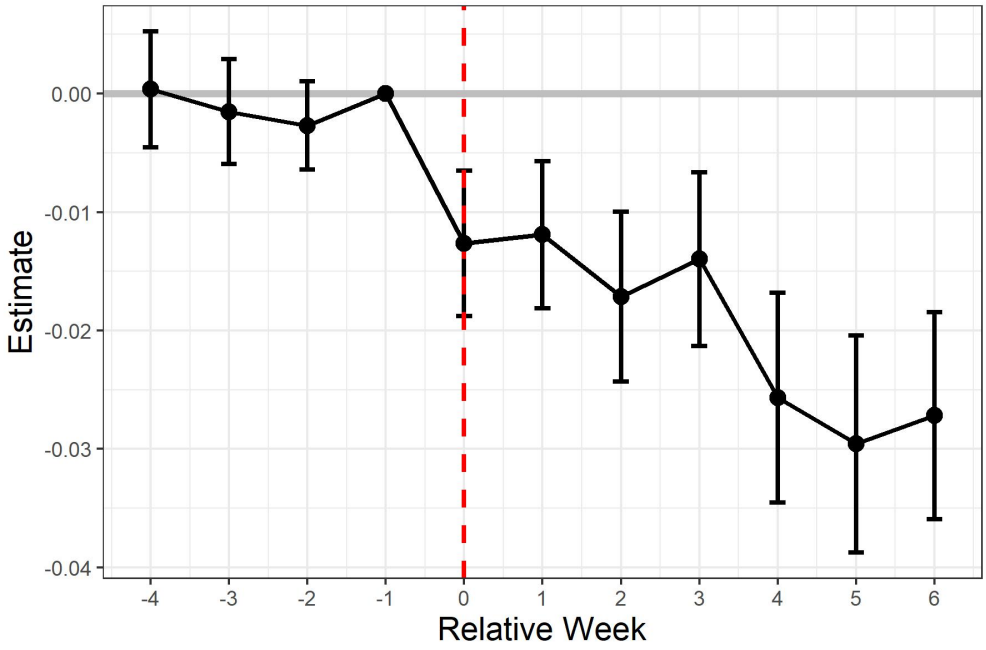
Note: Robust standard errors clustered at user level in parentheses. The unit of observation is user-app-week. The dependent variable is log numer of sessions. Post is an indicator variable which denotes if the time period is after the Dobbs verdict was leaked. mHealth App indicates whether the app is a mobile health app or a control app (Games).
$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.

Overall, our results suggest that the chilling effect on digital technology usage is significantly moderated by individual characteristics.

## 6.3 Other Privacy-Preserving Behavior

Finally, we also test for spillovers of the Dobbs ruling on the increase in privacy-preserving behavior in our sample of users who have ever used privacy-preserving browser apps during the sample period. In this analysis, we use the specification in Equation 1, but change the

Figure 2: Event Study Estimates - Alternate Controls




Note: The figure shows event study estimates of mobile health app usage relative to alternate control app usage. The dependent variable is the log number of weekly sessions. The unit of observation is at the user-app-week level. 95% confidence intervals are shown.

outcome variable to the usage of privacy-preserving browser apps (Brave, DuckDuckGo, and Tor) as our outcome variable.

We test for the likelihood of using privacy-preserving browser apps relative to the likelihood of using the control app post the Dobbs ruling. Column (1) in Table 10 shows that, post the Dobbs ruling, the likelihood of using privacy-preserving browsers increased significantly. The results of columns (2) and (3) indicate that this increase is driven mostly by new adopters who had not used any of these browser apps in the pre-period. Our results, therefore, confirm hypotheses 4a and 4b

Table 8: Impact of Social Media and News on Usage of Mobile Health Apps

| Dependent Variable: | Log(Sessions) | | | | | |
|---|---|---|---|---|---|---|
| | Social Media | | News | | Low Cred News | |
| | High | Low | High | Low | High | Low |
| | (1) | (2) | (3) | (4) | (5) | (6) |
| *Variables* | | | | | | |
| Post × mHealth App | -0.110*** | -0.072*** | -0.099*** | -0.086*** | -0.111*** | -0.074*** |
| | (0.017) | (0.014) | (0.018) | (0.013) | (0.016) | (0.015) |
| User Fixed Effect | Yes | Yes | Yes | Yes | Yes | Yes |
| App Fixed Effect | Yes | Yes | Yes | Yes | Yes | Yes |
| Week Fixed Effect | Yes | Yes | Yes | Yes | Yes | Yes |
| $R^2$ | 0.03178 | 0.02270 | 0.02923 | 0.02411 | 0.02610 | 0.02666 |
| Observations | 5,056,260 | 4,425,124 | 4,676,144 | 4,805,240 | 4,568,564 | 4,912,820 |

Note: Robust standard errors clustered at user level in parentheses. The unit of observation is user-app-week. The dependent variable is log numer of sessions. Post is an indicator variable which denotes if the time period is after the Dobbs verdict was leaked. mHealth App indicates whether the app is a mobile health app or a control app.
$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.

# 7 Discussion

In this paper, we study the impact of chilling effects on the usage of mobile health apps. Studying the privacy concerns surrounding the collection and storage of digital health data by technology firms is extremely important. Mobile health apps are very popular, but there is no overall federal regulatory structure for them. Wearable devices collect granular information about every aspect of a user's life, including their location, heart rate, stress levels, and reproductive health. This information is not protected by current patient privacy standards like HIPAA (Langley, 2014). Our results show that post-Dobbs, there was a large decrease in the use of mobile health apps, and this was especially higher among women. Data from mobile health apps and wearables are now increasingly used in legal proceedings. The large chilling effect is likely due to increased media and public scrutiny of how data from

Table 9: Impact of Dobbs on Usage of Mobile Health Apps

| Dependent Variable: | Log(Sessions) | | | | | |
|---|---|---|---|---|---|---|
| | Race | | Age | | Income | |
| | White | Non-White | <= 45 Yrs | > 45 Yrs | <$ 50,000 | >=$ 50,000 |
| | (1) | (2) | (3) | (4) | (5) | (6) |
| *Variables* | | | | | | |
| Post × mHealth App | -0.108*** | -0.088*** | -0.114*** | -0.071*** | -0.138*** | -0.068*** |
| | (0.015) | (0.020) | (0.018) | (0.013) | (0.020) | (0.013) |
| User Fixed Effect | Yes | Yes | Yes | Yes | Yes | Yes |
| App Fixed Effect | Yes | Yes | Yes | Yes | Yes | Yes |
| Week Fixed Effect | Yes | Yes | Yes | Yes | Yes | Yes |
| $R^2$ | 0.02574 | 0.02780 | 0.02811 | 0.02640 | 0.02340 | 0.02945 |
| Observations | 5,995,792 | 2,610,608 | 4,697,660 | 4,783,724 | 3,779,644 | 5,120,808 |

Note: Robust standard errors clustered at user level in parentheses. The unit of observation is user-app-week. The dependent variable is log total time. Post is an indicator variable which denotes if the time period is after the Dobbs verdict was leaked. mHealth App indicates whether the app is a mobile health app or a control app.
$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.

fitness apps could potentially be used by governments. Our results show that awareness is indeed a large moderating effect, as we find a larger decrease in usage among users with higher exposure to news and social media before the shock. Our results also show how users significantly increase their privacy-preserving behavior post-Dobbs, with the increase driven by first-time users.

Our findings have significant implications for the field of information systems. Mobile health technologies are a $480 billion market in the US, with one in every five Americans using a wearable fitness tracker. Mobile health technologies have proven benefits in improving self-management of health and can have an outsized impact on public health. However, the adoption and usage of these devices are conditional on the trust that users place in these systems and their willingness to share millions of data points in exchange for personalized recommendations to improve health. We show that despite the benefits available from mobile

Table 10: Impact of Dobbs on Usage of Web-Browser Apps

| Dependent Variable: | Likelihood of Usage | | |
|---|---|---|---|
| | All Users | Pre-Period Adopters | Pre-Period Non-Adopters |
| | (1) | (2) | (3) |
| *Variables* | | | |
| Post × Browser App | 0.024** | 0.006 | 0.055*** |
| | (0.010) | (0.013) | (0.017) |
| User Fixed Effect | Yes | Yes | Yes |
| App Fixed Effect | Yes | Yes | Yes |
| Week Fixed Effect | Yes | Yes | Yes |
| $R^2$ | 0.16228 | 0.18647 | 0.12052 |
| Observations | 11,572 | 7,304 | 4,268 |

Note: Robust standard errors clustered at user level in parentheses. The unit of observation is user-app-week. The dependent variable is an indicator variable which takes a value of 1 if the user used an app in a given week and 0 otherwise. Post is an indicator variable which denotes if the time period is after the Dobbs verdict was leaked. Browser App indicates whether the app is privacy preserving browser app or a control app.
$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.

health apps, shock to privacy expectations and ambiguity in how personal digital data is handled across different states with different restrictions on reproductive health, can have a large impact on the usage of these apps, particularly among women. Audit studies of mobile health apps, particularly FemTech apps, underscore the lack of consistency in privacy guidelines and data-sharing practices in these apps. We are the first in the literature to show that the lack of industry standards in privacy protections can negatively affect the usage of mobile health apps when consumers worry that their data might be shared with government agencies, regardless of whether these data are actually shared with the government. Such chilling effects can be detrimental to the expansion of one of the fastest growing sectors in

the technology industry.

The legalities of digital surveillance and the ability of police and prosecutors to access and use digital data in prosecutions are being heavily scrutinized in courts across the United States. In the landmark case Carpenter v. United States (Carpenter, 2016), the court ruled that individuals have a reasonable expectation of privacy from their phone companies, setting a legal precedent on how digital data should be obtained by the government. Since then, contextual applications of the Carpenter ruling have played out in many interpretations in courts around the U.S. on what constitutes a reasonable expectation of privacy and whether other forms of digital data, like search queries and digital visits, are protected under the Carpenter ruling (Conti-Cook, 2020). Data obtained from a user's digital devices, such as wearables, can reveal a lot about their interests and curiosities, and their admissibility in court is based on contested interpretations of the Carpenter protections. This suggests the need for policy guidance from legislators on how digital health records collected by mobile health apps fit into existing frameworks of digital health privacy and in creating protections from surveillance.

Our results also speak to the importance of privacy in the privacy vs. personalization debate. This balance has been studied in the information systems literature. Mobile health technologies and fitness trackers have been shown to be particularly effective in influencing positive changes in behavior and clinical outcomes through personalization and gamification, thus improving adherence and compliance to clinical recommendations (Rowland et al., 2020; Perski et al., 2017). Almost all mobile health technologies use some form of AI to achieve personalization. The scale and growth of these devices suggest that consumers reap great benefits from personalization. However, our results suggest that chilling effects due to fear of prosecution override the benefits of personalization. More specifically, the increased publicity about instances of states using digital data to prosecute women brought US citizens' digital health data within the realm of potential government surveillance.

This is especially true among women's usage of apps meant to help them track and manage their reproductive health. The Dobbs decision had an outsized negative impact on the usage of FemTech apps, with over a 60% drop in the usage of FemTech apps. This can have a downstream impact on women's entrepreneurship. Interestingly, a recent study by McKinsey shows how 70 percent of FemTech apps have at least one woman co-founder compared to only 20 percent of any new firm (Kemble et al., 2022). Further, Koning et al. (2021) find that female inventor teams are 35% more likely to focus on female-focused inventions. Chilling effects due to changes in public policy may affect the demand for female-focused technology inventions and reduce investment in technologies focused on women's health.

Our study is not without limitations. First, our data contains information only from mobile devices, which prevents us from studying interactions that occur through PCs. However, most mobile health apps are accessible only through phones to connect to wearable devices, and our results are robust to the choice of other control groups. Second, our sample is limited to about 1322 users. While the granular session-level data provides a deep understanding of the users' activities, we are not able to conduct analyses at the state level because of power limitations by splitting the sample further. It might be interesting to study the impact of self-censoring based on a person's state and the coverage of digital health data in local news for future work in this area. Despite these limitations, our study has important implications for policy makers and managers alike on how sensitive digital data collected from mobile apps should be handled.

# References

Adjerid, Idris, Alessandro Acquisti, Rahul Telang, Rema Padman, Julia Adler-Milstein. 2016. The impact of privacy regulation and technology incentives: The case of health information exchanges. *Management Science* **62**(4) 1042–1063.

Adler-Milstein, Julia, Joseph Kvedar, David W Bates. 2014. Telehealth among us hospitals: several factors, including state reimbursement and licensure policies, influence adoption. *Health Affairs* **33**(2) 207–215.

Agarwal, Ritu, Michelle Dugas, Guodong Gao, PK Kannan. 2020. Emerging technologies and analytics for a new era of value-centered marketing in healthcare. *Journal of the Academy of Marketing Science* **48** 9–23.

Agarwal, Saharsh, Deepa Mani, Rahul Telang. 2023. The impact of ride-hailing services on congestion: Evidence from indian cities. *Manufacturing & Service Operations Management* .

Agarwal, Saharsh, Ananya Sen. 2022. Antiracist curriculum and digital platforms: Evidence from black lives matter. *Management Science* **68**(4) 2932–2948.

Anderson, Michaela R, Gordon Burtch, Brad N Greenwood. 2024. The impact of abortion restrictions on american mental health. *Science Advances* **10**(27) eadl5743.

Andreoli, Virginia A, Stephen Worchel, Robert Folger. 1974. Implied threat to behavioral freedom. *Journal of Personality and Social Psychology* **30**(6) 765.

Aramendi, Ane Alberdi, Alyssa Weakley, Asier Aztiria Goenaga, Maureen Schmitter-Edgecombe, Diane J Cook. 2018. Automatic assessment of functional health decline in older adults based on smart home data. *Journal of biomedical informatics* **81** 119–130.

Aronson, Samuel J, Heidi L Rehm. 2015. Building the foundation for genomics in precision medicine. *Nature* **526**(7573) 336–342.

Autor, David H. 2003. Outsourcing at will: The contribution of unjust dismissal doctrine to the growth of employment outsourcing. *Journal of labor economics* **21**(1) 1–42.

Ayabakan, Sezgin, Indranil R Bardhan, Zhiqiang Zheng. 2024. Impact of telehealth and

process virtualization on healthcare utilization. *Information Systems Research* **35**(1) 45–65.

Baker-White, Emily, Sarah Emerson. 2022. Facebook gave nebraska cops a teen's dms. they used them to prosecute her for having an abortion. Tech. rep. URL `https://www.forbes.com/sites/emilybaker-white/2022/08/08/facebook-abortion-teen-dms/`.

Bardhan, Indranil, Hsinchun Chen, Elena Karahanna. 2020. Connecting systems, data, and people: A multidisciplinary research roadmap for chronic disease management. *MIS Quarterly* **44**(1).

Bardhan, Indranil R, Mark F Thouin. 2013. Health information technology and its impact on the quality and cost of healthcare delivery. *Decision Support Systems* **55**(2) 438–449.

Bates, David W, Adam Landman, David M Levine. 2018. Health apps and health policy: what is needed? *Jama* **320**(19) 1975–1976.

Bergström, Annika. 2015. Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in human behavior* **53** 419–426.

Bestsennyy, Oleg, Greg Gilbert, Alex Harris, Jennifer Rost, et al. 2021. Telehealth: a quarter-trillion-dollar post-covid-19 reality. *McKinsey & Company* **9**.

Blank, Grant, Gillian Bolsover, Elizabeth Dubois. 2014. A new privacy paradox: Young people and privacy on social network sites. *Prepared for the Annual Meeting of the American Sociological Association*, vol. 17.

Brandimarte, Laura, Alessandro Acquisti, George Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social psychological and personality science* **4**(3) 340–347.

Brehm, Jack W. 1966. A theory of psychological reactance .

Brehm, Sharon S, Jack W Brehm. 2013. *Psychological reactance: A theory of freedom and*

*control*. Academic Press.

Brohman, Kathryn, Shamel Addas, Jeff Dixon, Alain Pinsonneault. 2020. Cascading feedback: A longitudinal study of a feedback ecosystem for telemonitoring patients with chronic disease. *MIS Quarterly* **44**(1).

Buckman, Joseph R, Idris Adjerid, Catherine Tucker. 2023. Privacy regulation and barriers to public health. *Management Science* **69**(1) 342–350.

Carpenter, Timothy. 2016. Carpenter v. united states .

Carr Smyth, Julie. 2023. A black woman was criminally charged after a miscarriage. it shows the perils of pregnancy post-roe. Tech. rep. URL `https://apnews.com/techreport/ohio-miscarriage-prosecution-brittany-watts-b8090abfb5994b8a23457b80cf3f27ce`.

Chellappa, Ramnath K, Raymond G Sin. 2005. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management* **6** 181–202.

Chib, Arul, Sapphire H Lin. 2018. Theoretical advancements in mhealth: a systematic review of mobile apps. *Journal of health communication* **23**(10-11) 909–955.

Collier, Kevin, Minyvonne Burke. 2022. Facebook turned over chat messages between mother and daughter now charged over abortion. Tech. rep. URL `https://www.nbcnews.com/tech/tech-news/facebook-turned-chat-messages-mother-daughter-now-charged-abortion-rcna42185`.

Conti-Cook, Cynthia. 2020. Surveilling the digital abortion diary. Tech. rep.

Cox, Joseph. 2022a. Data broker is selling location data of people who visit abortion clinics. Tech. rep. URL `https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood`.

Cox, Joseph. 2022b. Data broker is selling location data of people who visit abortion clinics. Tech. rep. URL https://www.vice.com/en/techreport/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

Cox, Joseph. 2022c. Data broker safegraph stops selling location data of people who visit planned parenthood. Tech. rep. URL https://www.vice.com/en/techreport/88gyn5/data-broker-safegraph-stops-selling-location-data-of-people-who-visit-planned-parenthood.

Earle, Sarah, Hannah R Marston, Robin Hadley, Duncan Banks. 2020. Use of menstruation and fertility app trackers: a scoping review of the evidence. *BMJ sexual & reproductive health* .

Edelson. 2022. Post-dobbs, your private data will be used against you. Tech. rep. URL https://news.bloomberglaw.com/us-law-week/post-dobbs-your-private-data-will-be-used-against-you.

Epstein, Daniel A, Nicole B Lee, Jennifer H Kang, Elena Agapie, Jessica Schroeder, Laura R Pina, James Fogarty, Julie A Kientz, Sean Munson. 2017. Examining menstrual tracking to inform the design of personal informatics tools. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 6876–6888.

Estrin, Deborah, Ida Sim. 2010. Open mhealth architecture: an engine for health care innovation. *Science* **330**(6005) 759–760.

Fazio, Lisa K, Nadia M Brashier, B Keith Payne, Elizabeth J Marsh. 2015. Knowledge does not protect against illusory truth. *Journal of experimental psychology: general* **144**(5) 993.

Ferguson, Andrew Guthrie. 2017. The rise of big data policing: Surveillance, race, and the future of law enforcement. *The Rise of Big Data Policing*. New York University Press.

Ferretti, Agata, Elettra Ronchi, Effy Vayena. 2019. From principles to practice: benchmarking government guidance on health apps. *The Lancet Digital Health* **1**(2) e55–e57.

Fitzpatrick, Jen. 2022. Protecting people's privacy on health topics. Tech. rep. URL `https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/`.

Frik, Alisa, Juliann Kim, Joshua Rafael Sanchez, Joanne Ma. 2022. Users' expectations about and use of smartphone privacy and security settings. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–24.

Gambier-Ross, Katie, David J McLernon, Heather M Morgan. 2018. A mixed methods exploratory study of women's relationships with and uses of fertility tracking apps. *Digital Health* **4** 2055207618785077.

Ghose, Anindya, Xitong Guo, Beibei Li, Yuanyuan Dang. 2022. Empowering patients using smart mobile health platforms: Evidence of a randomized field experiment. *Management Information Systems Quarterly* **46**(1) 151–192.

Ghose, Anindya, Beibei Li, Meghanath Macha, Chenshuo Sun, Natasha Ying Zhang Foutz. 2020. Trading privacy for the greater social good: How did america react during covid-19? *arXiv preprint arXiv:2006.05859* .

Gilman, Michele E. 2020. Five privacy principles (from the gdpr) the united states should adopt to advance economic justice. *Ariz. St. LJ* **52** 368.

Gilman, Michele Estrin. 2021. Periods for profit and the rise of menstrual surveillance. *Colum. J. Gender & L.* **41** 100.

Goldfarb, Avi, Catherine Tucker. 2019. Digital economics. *Journal of economic literature* **57**(1) 3–43.

Goldfarb, Avi, Catherine E Tucker. 2011. Privacy regulation and online advertising. *Management science* **57**(1) 57–71.

Greenwood, Brad N, Ritu Agarwal. 2016. Matching platforms and hiv incidence: An empirical investigation of race, gender, and socioeconomic status. *Management Science* **62**(8) 2281–2303.

Gross, Paige. 2024. Data privacy after dobbs: Is period tracking safe? Tech. rep. URL `https://kansasreflector.com/2024/07/28/data-privacy-after-dobbs-is-period-tracking-safe/`.

Guo, Xitong, Yongqiang Sun, Ziyu Yan, Nan Wang. 2012. Privacy-personalization paradox in adoption of mobile health service: the mediating role of trust .

Heerden, Alastair van, Mark Tomlinson, Leslie Swartz. 2012. Point of care in your pocket: a research agenda for the field of m-health. *Bulletin of the World Health Organization* **90** 393–394.

Hensher, Martin, Paul Cooper, Sithara Wanni Arachchige Dona, Mary Rose Angeles, Dieu Nguyen, Natalie Heynsbergh, Mary Lou Chatterton, Anna Peeters. 2021. Scoping review: development and assessment of evaluation frameworks of mobile health apps for recommendations to consumers. *Journal of the American Medical Informatics Association* **28**(6) 1318–1329.

Hill, Kashmir. 2022. Deleting your period tracker won't protect you. Tech. rep. URL `https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html`.

Hutton, Luke, Blaine A Price, Ryan Kelly, Ciaran McCormick, Arosha K Bandara, Tally Hatzakis, Maureen Meadows, Bashar Nuseibeh, et al. 2018. Assessing the privacy of mhealth apps for self-tracking: heuristic evaluation approach. *JMIR mHealth and uHealth*

**6**(10) e9217.

Jiang, Jinglu, Ann-Frances Cameron. 2020. It-enabled self-monitoring for chronic disease self-management: An interdisciplinary review. *MIS quarterly* **44**(1).

Joh, Elizabeth. 2022. The potential overturn of roe shows why we need more digital privacy protections. Tech. rep. URL `https://slate.com/technology/2022/05/roe-overturn-data-privacy-laws.html`.

Johnson, Kevin B, Wei-Qi Wei, Dilhan Weeraratne, Mark E Frisse, Karl Misulis, Kyu Rhee, Juan Zhao, Jane L Snowdon. 2021. Precision medicine, ai, and the future of personalized health care. *Clinical and translational science* **14**(1) 86–93.

Jr, Clint Cowan. 2017. Data privacy concerns make the post-roe era uncharted territory. Tech. rep. URL `https://www.butlersnow.com/wp-content/uploads/2017/07/Wearable-Technology-Discovery-In-Personal-Injury-Cases.pdf`.

Kasakowskij, Regina, Thomas Kasakowskij, Kaja Fietkiewicz. 2020. Pinterest: A unicorn among social media? an investigation of the platform's quality and specifications. *ECSM 2020 8th European Conference on Social Media*. Academic Conferences and publishing limited, 399.

Kemble, Emma, Lucy Pérez, Valentina Sartori, Gila Tolub, Alice Zheng. 2022. The dawn of the femtech revolution. Tech. rep., McKinsey and Company. URL `https://www.mckinsey.com/industries/healthcare/our-insights/the-dawn-of-the-femtech-revolution`.

Kim. 2022. Data privacy concerns make the post-roe era uncharted territory. Tech. rep. URL `https://www.npr.org/2022/07/02/1109565803/data-privacy-abortion-roe-apps`.

Koning, Rembrand, Sampsa Samila, John-Paul Ferguson. 2021. Who do we invent for? patents by women focus more on women's health, but few women get to invent. *Science*

**372**(6548) 1345–1348.

Lancaster, Karla, Aseel Abuzour, Manmeet Khaira, Annalise Mathers, April Chan, Vivian Bui, Annie Lok, Lehana Thabane, Lisa Dolovich. 2018. The use and effects of electronic health tools for patient self-monitoring and reporting of outcomes following medication use: systematic review. *Journal of medical Internet research* **20**(12) e294.

Langley, Matthew R. 2014. Hide your health: addressing the new privacy problem of consumer wearables. *Geo. LJ* **103** 1641.

Larson, Richard S. 2018. A path to better-quality mhealth apps. *JMIR mHealth and uHealth* **6**(7) e10414.

Lee, Lisa M, Lawrence O Gostin. 2009. Ethical collection, storage, and use of public health data: a proposal for a national privacy protection. *Jama* **302**(1) 82–84.

Li, Xiao-Bai, Xiaoping Liu, Luvai Motiwalla. 2021. Valuing personal data with privacy consideration. *Decision Sciences* **52**(2) 393–426.

Liu, Shuang, Jessica F Willoughby. 2018. Do fitness apps need text reminders? an experiment testing goal-setting text message reminders to promote self-monitoring. *Journal of health communication* **23**(4) 379–386.

Liu, Yizhi, Xuan Lu, Gang Zhao, Chengjiang Li, Junyi Shi. 2022. Adoption of mobile health services using the unified theory of acceptance and use of technology model: Self-efficacy and privacy concerns. *Frontiers in Psychology* **13** 944976.

Madden, Mary, Michele Gilman, Karen Levy, Alice Marwick. 2017. Privacy, poverty, and big data: A matrix of vulnerabilities for poor americans. *Wash. UL Rev.* **95** 53.

Magrabi, Farah, Ibrahim Habli, Mark Sujan, David Wong, Harold Thimbleby, Maureen Baker, Enrico Coiera. 2019. Why is it so difficult to govern mobile apps in healthcare?

*BMJ health & care informatics* **26**(1).

Marcolino, Milena Soriano, João Antonio Queiroz Oliveira, Marcelo D'Agostino, Antonio Luiz Ribeiro, Maria Beatriz Moreira Alkmim, David Novillo-Ortiz. 2018. The impact of mhealth interventions: systematic review of systematic reviews. *JMIR mHealth and uHealth* **6**(1) e8873.

Marthews, Alex, Catherine E Tucker. 2017. Government surveillance and internet search behavior. *Available at SSRN 2412564* .

Mathiason, Jessica Lee. 2023. Femtech: The" smart" business of menstruation, hormone tracking, and the corporate construction of risk. *Feminist Studies* **49**(1) 118–149.

McQuillan, Laura. 2022. Americans are being urged to delete period tracking apps. should canadians do the same? Tech. rep. URL `https://www.cbc.ca/news/health/period-tracker-apps-data-privacy-1.6510029`.

Mehrnezhad, Maryam, Laura Shipp, Teresa Almeida, Ehsan Toreini. 2022. Vision: Too little too late? do the risks of femtech already outweigh the benefits? *Proceedings of the 2022 European Symposium on Usable Security*. 145–150.

Mehta, Mehul C, Ingrid T Katz, Ashish K Jha. 2020. Transforming global health with ai. *New England Journal of Medicine* **382**(9) 791–793.

Miller, Amalia R, Catherine Tucker. 2009. Privacy protection and technology diffusion: The case of electronic medical records. *Management science* **55**(7) 1077–1093.

Miller, Amalia R, Catherine Tucker. 2018. Privacy protection, personalized medicine, and genetic testing. *Management Science* **64**(10) 4648–4668.

Mittal, Sudip, Neha Gupta, Prateek Dewan, Ponnurangam Kumaraguru. 2013. The pin-bang theory: Discovering the pinterest world. *arXiv preprint arXiv:1307.4952* .

Murphy, Margi. 2022. Anti-abortion centers find pregnant teens online, then save their data. Tech. rep. URL https://www.bloomberg.com/news/techreports/2022-06-27/anti-abortion-centers-find-pregnant-teens-online-then-save-their-data.

Nelson, Sophie L. 2024. The post-dobbs reality: Privacy expectations for period-tracking apps in criminal abortion prosecutions. *Pepperdine Law Review* **51**(4) 783–820.

Ng, Andy H, Mohammad S Kermani, Richard N Lalonde. 2021. Cultural differences in psychological reactance: Responding to social media censorship. *Current Psychology* **40** 2804–2813.

O'neil, Cathy. 2017. *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.

Ottoni, Raphael, Joao Paulo Pesce, Diego Las Casas, Geraldo Franciscani Jr, Wagner Meira Jr, Ponnurangam Kumaraguru, Virgilio Almeida. 2013. Ladies first: Analyzing gender roles and behaviors in pinterest. *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 7. 457–465.

Penney, Jon. 2017. Internet surveillance, regulation, and chilling effects online: A comparative case study. *Regulation, and Chilling Effects Online: A Comparative Case Study (May 27, 2017)* **6**(2).

Pennycook, Gordon, Tyrone D Cannon, David G Rand. 2018. Prior exposure increases perceived accuracy of fake news. *Journal of experimental psychology: general* **147**(12) 1865.

Pennycook, Gordon, David G Rand. 2021. The psychology of fake news. *Trends in cognitive sciences* **25**(5) 388–402.

Perski, Olga, Ann Blandford, Robert West, Susan Michie. 2017. Conceptualising engagement with digital behaviour change interventions: a systematic review using principles from

critical interpretive synthesis. *Translational behavioral medicine* **7**(2) 254–267.

Pleasure, Zoe H, Andréa Becker, Dana M Johnson, Kathleen Broussard, Laura Lindberg. 2024. How tiktok is being used to talk about abortion post-roe: A content analysis of the most liked abortion tiktoks. *Contraception* **133** 110384.

Pop-Eleches, Cristian, Harsha Thirumurthy, James P Habyarimana, Joshua G Zivin, Markus P Goldstein, Damien De Walque, Leslie Mackeen, Jessica Haberer, Sylvester Kimaiyo, John Sidle, et al. 2011. Mobile phone technologies improve adherence to antiretroviral treatment in a resource-limited setting: a randomized controlled trial of text message reminders. *Aids* **25**(6) 825–834.

Potoglou, Dimitris, Fay Dunkerley, Sunil Patil, Neil Robinson. 2017. Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-european study. *Computers in Human Behavior* **75** 811–825.

Qiang, Christine Zhenwei, Masatake Yamamichi, Vicky Hausman, Daniel Altman, IS Unit. 2011. Mobile applications for the health sector. *Washington: World Bank* **2**.

Radivojevic, Kristina, Nicholas Clark, Anna Klempay, Paul Brenner. 2024. Defending novice user privacy: An evaluation of default web browser configurations. *Computers & Security* **140** 103784.

Reddy, Monika, Peter Pesl, Maria Xenou, Christofer Toumazou, Desmond Johnston, Pantelis Georgiou, Pau Herrero, Nick Oliver. 2016. Clinical safety and feasibility of the advanced bolus calculator for type 1 diabetes based on case-based reasoning: a 6-week nonrandomized single-arm pilot study. *Diabetes technology & therapeutics* **18**(8) 487–493.

Righney, Meghan A. 2019. Data privacy concerns make the post-roe era uncharted territory. Tech. rep. URL `https://www.americanbar.org/groups/litigation/resources/newsletters/products-liability/steps-for-discovery-subpoenaing-wearable-techn`

ology-data/.

Riley, Sarah, Klara Paskova. 2022. A post-phenomenological analysis of using menstruation tracking apps for the management of premenstrual syndrome. *Digital health* **8** 20552076221144199.

Rosso, Mark, ABM Nasir, Mohsen Farhadloo. 2020. Chilling effects and the stock market response to the snowden revelations. *New Media & Society* **22**(11) 1976–1995.

Rowland, Simon P, J Edward Fitzgerald, Thomas Holme, John Powell, Alison McGregor. 2020. What is the clinical value of mhealth for patients? *NPJ digital medicine* **3**(1) 4.

Samory, Mattia, Tanushree Mitra. 2018. 'the government spies using our webcams' the language of conspiracy theories in online discussions. *Proceedings of the ACM on Human-Computer Interaction* **2**(CSCW) 1–24.

Schauer, Frederick. 1978. Fear, risk and the first amendment: Unraveling the chilling effect. *BUL rev.* **58** 685.

Scott, Karen, Deborah Richards, Rajindra Adhikari, et al. 2015. A review and comparative analysis of security risks and safety measures of mobile health apps. *Australasian Journal of Information Systems* **19**.

Sheppard, Maria K. 2020. mhealth apps: disruptive innovation, regulation, and trust—a need for balance. *Medical Law Review* **28**(3) 549–572.

Shipp, Laura, Jorge Blasco. 2020. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proc. Priv. Enhancing Technol.* **2020**(4) 491–510.

Silveira, Patrícia, Rolf Van De Langenberg, Eva van Het Reve, Florian Daniel, Fabio Casati, Eling D De Bruin. 2013. Tablet-based strength-balance training to motivate and improve adherence to exercise in independently living older people: a phase ii preclinical

exploratory trial. *Journal of medical Internet research* **15**(8) e159.

Sohda, Satoshi, Kenta Suzuki, Ichiro Igari. 2017. Relationship between the menstrual cycle and timing of ovulation revealed by new protocols: analysis of data from a self-tracking health app. *Journal of medical Internet research* **19**(11) e391.

Stopczynski, Kelli. 2015. Prosecutors: Text messages detail weeks leading up to patel's forced abortion. Tech. rep. URL `https://wsbt.com/news/local/prosecutors-text-messages-detail-weeks-leading-up-to-patels-forced-abortion`.

Stuart, Allyson Haynes. 2022. Privacy in discovery after dobbs. *Va. JL & Tech.* **26** 1.

Thibault, Denae. 2022. Flo, the leading female health app, launches 'anonymous mode' to further protect reproductive health information in wake of roe v. wade decision. Tech. rep. URL `https://flo.health/newsroom/flo-launches-anonymous-mode`.

Tomlinson, Mark, Mary Jane Rotheram-Borus, Leslie Swartz, Alexander C Tsai. 2013. Scaling up mhealth: where is the evidence? *PLoS medicine* **10**(2) e1001382.

Torchinsky, Rina. 2022. How period tracking apps and data privacy fit into a post-roe v. wade climate. Tech. rep. URL `https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps`.

Trau, Morgan. 2022. Period tracking app users delete app, citing privacy concerns after abortion banned in ohio. Tech. rep. URL `https://www.news5cleveland.com/news/politics/ohio-politics/period-tracking-app-users-delete-app-citing-privacy-concerns-after-abortion-banned-in-ohio`.

Tucker, Catherine E. 2014. Social networks, personalized advertising, and privacy controls. *Journal of marketing research* **51**(5) 546–562.

Walter, Carrie, Audrey Tsang. 2022. Patient data privacy at clue: A statement from the

co-ceos. Tech. rep. URL https://helloclue.com/techreports/about-clue/patient-data-privacy-at-clue-a-statement-from-the-co-ceos.

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

Wright, Jasmine, Maegan Vazquez. 2022. White house says americans should be 'really careful' about using period tracker apps. Tech. rep. URL https://www.cnn.com/2022/07/08/politics/white-house-period-tracker-apps/index.html.

Zakrzewski, Cat, Pranshu Verma, Claire Parker. 2022. Texts, web searches about abortion have been used to prosecute women. Tech. rep. URL https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/.

Zhang, Sushen, Seyed Mojtaba Hosseini Bamakan, Qiang Qu, Sha Li. 2018. Learning for personalized medicine: a comprehensive review from a deep learning perspective. *IEEE reviews in biomedical engineering* **12** 194–208.

Zukowski, Tomasz, Irwin Brown. 2007. Examining the influence of demographic factors on internet users' information privacy concerns. *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*. 197–204.