

Routledge
Taylor & Francis Group

Journal of Women, Politics & Policy

ISSN: 1554-477X (Print) 1554-4788 (Online) Journal homepage: www.tandfonline.com/journals/wwap20

Tracking the Trackers: 'Menstruapp' Privacy Policies Following the *Dobbs* Decision

Katie Krumbholz, Alice Militaru & Kyle J. Morgan

To cite this article: Katie Krumbholz, Alice Militaru & Kyle J. Morgan (2024) Tracking the Trackers: 'Menstruapp' Privacy Policies Following the *Dobbs* Decision, Journal of Women, Politics & Policy, 45:1, 167-189, DOI: 10.1080/1554477X.2024.2300103

To link to this article: https://doi.org/10.1080/1554477X.2024.2300103

Published online: 21 Jan 2024.

Submit your article to this journal

Article views: 623

View related articles

View Crossmark data

Citing articles: 6 View citing articles

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=wwap20

JOURNAL OF WOMEN, POLITICS & POLICY
2024, VOL. 45, NO. 1, 167–189
https://doi.org/10.1080/1554477X.2024.2300103

Routledge
Taylor & Francis Group

Check for updates

Tracking the Trackers: 'Menstruapp' Privacy Policies Following the *Dobbs* Decision

Katie Krumbholz[a], Alice Militaru[a], and Kyle J. Morgan[b]

[a]Political Science, Rutgers, The State University of New Jersey, New Brunswick, New Jersey, USA; [b]Department of Political Science and Geography, Francis Marion University, Florence, South Carolina, USA

ABSTRACT

Reproductive rights have faced uncertainty following a succession of court decisions since 2021, particularly following the decision in Dobbs v. Jackson Woman's Health. This article explores the response from mobile applications dubbed "period trackers" or "menstruapps," which allow individuals to track their menstrual cycles on mobile devices. Following the *Dobbs* decision and subsequent efforts by states to criminalize abortion, there were many voices concerned about the data these apps collect. This paper analyzes the privacy policies from over 30 apps. Specifically, focusing on how these apps changed their language, or not, during a period when reproductive rights were under increased threat.

KEYWORDS

Abortion; reproductive rights; privacy; technology; mobile applications

Introduction

For over a decade, period tracker applications have been available for those who menstruate to record the start of their cycles, symptoms, use of birth control, ovulation dates, and more (Worsfold et al. 2021). A 2019 Kaiser Family Foundation survey reported that approximately 1/3rd of women in the United States used a period tracking application (KFF 2019), frequently referred to as "femtech" or "menstruapps." As the number and use of these apps has grown, menstruapp users find themselves at a familiar crossroads – share personal information with technology to make your life easier but surrender control over who has access to that data. This trade-off is not new; our daily lives require us to give up more and more information to tech companies in the name of conveniences.

However, the data collected via these applications is particularly relevant in the aftermath of the decision in *Dobbs v. Jackson Women's Health Organization* and other recent changes to reproductive rights. Since the *Dobbs* decision, 14 states have moved to ban abortion and 10 more are in the process of doing so or are looking to do so in the near future (Nash and Guarnieri 2023; New York Times 2023). In 2020 while reproductive rights were under threat, abortion was not criminalized; however, Texas' SB8 and a number of other copycat state laws[1] not only sought to criminalize abortion but also to target providers and/or those aiding pregnant individuals in getting an abortion. The data collected by menstruapps is thus especially relevant in this context. Surveillance of pregnant individuals is not new (Flavin 2010; Goodwin 2020; Howard 2020; Ziegler 2014), but as technology and data capitalism creep into more and more areas of what were once private and personal, and we see increasing efforts to criminalize abortion and reproductive healthcare, this surveillance and the data held by companies must be viewed and considered in a different light (Citron 2022; Zuboff 2019).

Data collected by menstruapps can show pauses in a normal cycle which can be indicative of a pregnancy and a return of a cycle, potentially signaling the end of that pregnancy. Even more concerning, the location tracking these applications are capable of can show that users were

CONTACT Kyle J. Morgan Kyle.Morgan@fmarion.edu Department of Political Science and Geography, Francis Marion University, 4822 E. Palmetto St, Florence, SC 29506, USA

© 2024 Taylor & Francis Group, LLC

present at an abortion clinic (Torchinsky 2022). While to date there have been no documented cases where the data contained in a menstruapp was used against someone, the risk this data poses has been subject to a great deal of attention in the media.[2] Following the Dobb's decision there were a number of voices urging users to delete these apps from their phones, cautioning that the data could be used against the user. Ironically, despite these warnings, downloads of these applications have since doubled (Hill 2023).

The surge of menstruapp downloads could come as a result of increased public fear – those who menstruate have an increased need to track periods, especially as states narrow the window for seeking a legal abortion. However, this also highlights the double bind in which individuals are placed. Menstruapps present a convenient way to track that information and to be informed about one's health, empowering individuals to make choices and control their reproductive lives. At the same time, through their intended use individuals are, in theory, putting themselves at legal risk. While users could return to pen and paper, the popularity of these applications speaks to their convenience. But adding this additional layer of legal risk changes the conversation around data capitalism and the choices individuals make between privacy and convenience.

This all raises an important question as to how, if at all, these companies responded to the *Dobbs* decision and the broader changing landscape of reproductive rights during this period. The data these companies collect sits at a complicated intersection, where on one hand they are marketed as empowering individuals through said data,[3] and on the other hand that same data has been flagged by activists as endangering their users (Garamvolgyi 2022; Hamilton and Reuter 2022; Morrison 2022). Further, since we are discussing private businesses, there is the omni-present question of profit. These competing considerations make analyzing privacy policies during this period particularly interesting and important. Broadly speaking, companies claim that privacy policies serve two purposes; outlining what data is collected when one uses an application or program and also what rights the user is entitled to regarding the use, deletion, or sharing of that data.

What is especially interesting to understand is the response (or lack thereof) of menstruapp companies. Changes to privacy policies in response to the overturning of *Roe v. Wade* are relevant both because of the potential impact on users and because it sheds light on the impact of Supreme Court Decisions on non-government entities. We think that examining how privacy policy language changed across different companies, either to protect user data or deny those protections, is important to include in the conversation of reproductive rights following *Dobbs*. We also note that it is just the beginning of measuring the impact of *Dobbs* and its effect on matters of privacy and health.

The conversation surrounding not just these, but all types of applications and their privacy policies goes far beyond the abortion debate. Menstruapps are just one example of the conversation surrounding mass data collection and how that has evolved. As states have begun to criminalize abortion, data women have given up freely for years and which did not pose a legal threat before June 24, 2022, can now, possibly, be turned against them. We conclude based on our analysis that this is because the "privacy policy" which gives the illusion of protecting the user is instead designed to protect the companies as they profit off that data.

Digital blind spots: surveillance capitalism's role in menstruapps nonresponse to *Dobbs v. Jackson Woman's Health Organization*

Our analysis is situated among several rich literatures. First, whether the Supreme Court holds sway is much debated, particularly with respect to its influence on lower courts, other branches of government, and general public opinion. Here we go in a unique direction and question its influence on private actors (the companies behind the menstruapps), asking if they respond to Supreme Court decisions (i.e., *Dobbs*) by changing their privacy policies. However, this question is muddied by a further question – what is the purpose of these privacy policies? To understand this, we must draw from two additional literatures – one involving the question of a right to privacy, and another the question of reproductive rights in an age of surveillance capitalism. Is the purpose of the privacy

policies to protect their users, specifically, women of reproductive age? If so, is that reflected via updates to the policy as to how their sensitive data will be protected from authorities who may want to use it to prosecute those who they suspect of obtaining illegal abortions? Or is the purpose of the privacy policy simply to protect the company from any sort of liability? In this case, we might expect to see changes which add disclaimers about complying with law enforcement – or no changes at all if that verbiage already exists.

Courts and abortion providers

Rosenberg (1991) looks at the impact of the Court's decision in *Roe* on abortions sought in the US. Leading with data on the number of abortions performed in the US over time, he argues that abortion was already significantly increasing as early as 1970, three years prior to *Roe*. He also argues that other numbers fail to show any impact of *Roe* such as the number of hospitals providing abortions and the percentage of women traveling out of state to obtain an abortion. Additionally, immediately after the Court ruled on *Roe*, state legislatures began to test its limits and lower courts were inconsistent in their adherence to the ruling (Nash and Donovan 2019; Siegel 1992; Ziegler 2014). This, along with the increasingly polarized public opinion on "discretionary" abortions (Franklin and Kosaki 1989; Pew Research Center 2022), left an opening for those opposing abortion to chip away at *Roe* using a variety of tactics (Brown 2004; Collett 2003; Halva-Neubauer and Zeigler 2010; Roberti 2022).

Rosenberg (1991) does, however, find an impact in the same place we are looking: among private actors. The number of abortion *providers*, specifically abortion clinics, increased by 113% in the three years after *Roe* (Rosenberg 1991). He quotes legal activist Janice Goodman who says, "some doctors are going to see a very substantial amount of money to be made on this" (Rosenberg 1991, 198). So yes, *Roe* had an impact, but one that was motivated by economics rather than the protection of women. This foreshadows the answer to our question about whether the companies behind menstruapps are actually interested in protecting women or their own interests. The policy of only one company we analyzed stood in contrast to all the others. This particular company analyzed, collected, and stored user data in such a way that protected the user, but also prevented them from profiting off the data. The remaining companies had policies that were ambiguous about how and when users could delete data, or even if they could do so at all. The language in these privacy policies suggests that the companies behind them are motivated by profits built upon the data collected from users because the policies are written in a way that protects the companies rather than the users themselves.

Courts and privacy

The question of a right to privacy stretches back over a century, raised in the classic Harvard Law Review Article by Brandeis and Warren (1890). They were alarmed by infringements on privacy and argued for a "right to be left alone" (Brandeis and Warren 1890). The right to privacy, however, is deeply linked to reproductive rights. The right to privacy was first recognized by the US Supreme Court in *Griswold v. Connecticut*, a case specifically about reproductive rights, and thus in the United States questions of privacy and reproductive rights have been inextricably linked. In *Griswold* (381), the right to privacy is introduced as a "peripheral right" that existed in the "penumbras" of other, explicit rights. The First, Third, Fourth, Fifth, and Ninth Amendments are all cited as creating a "zone of privacy." The Supreme Court used this peripheral right to privacy to defend, not the use of contraceptives, but the "sacred precincts of marital bedrooms" and the "privacy surrounding the marriage relationship." The use of contraceptives was protected by the right to use them *privately* rather than an absolute right to use them.

Seven years later, the *Roe v. Wade* (113) decision would strengthen the link between privacy and reproductive rights as the right to privacy was found, "broad enough to encompass a woman's decision whether or not to terminate her pregnancy." *Roe* extended the right to privacy from something afforded by the sanctity of marriage to a personal right; privacy no longer required two people.

However, in *Roe* (113), the Court also notes that the right to privacy is by no means absolute – "the woman's privacy is no longer sole and any right of privacy she possesses must be measured accordingly." The woman's privacy is not sole, because it is shared with the fetus instead of the husband.

Bellotti v. Baird (622) then extends the right to privacy with respect to abortion to minors, justifying this decision by explaining that the urgent nature of the decision to terminate a pregnancy and the fact that minors are "particularly vulnerable to their parents' efforts to obstruct both an abortion and their access to court." In order to protect the right to an abortion, the Court protected the right to keep that abortion confidential. While the decision for *Bellotti v. Baird* was being written in 1979, 29 states had already put into place laws that allowed minors to acquire contraception confidentially (Myers 2022). This question of age is relevant to the analysis of the privacy policies as the right to delete data varied based on age. For example, some apps stated that minors under 13 who used their app would be able to request to have their deleted immediately while others set the age at 16 or under.[4]

In 2001, *Ferguson v. City of Charleston* reckoned with the medical privacy of pregnant women. The Medical University of South Carolina began drug testing pregnant women with the intention of prosecuting those using illegal substances during pregnancy. The Court found this drug testing to constitute an unreasonable search based in the "reasonable expectation of privacy enjoyed by the typical patient" (10). Pregnant women could expect that the results of any diagnostic tests would not be "shared with nonmedical personnel without her consent" (10). The Court explicitly stated that because the purpose of the searches (drug tests) was to "generate evidence for law enforcement" (15), Fourth Amendment protections were activated and "prohibition against nonconsensual, warrantless, and suspicion-less searches" (18) applied to the drug testing of pregnant women. As such, *Ferguson* is particularly relevant to the discussion of menstruapp privacy protections.

These cases just scratch the surface of the case law surrounding abortion, privacy, and reproductive rights and are illustrative rather than exhaustive. Additionally, they do not consider the relationship between private businesses and individuals using contraception or abortion services. The right to privacy is much harder to define when individuals willingly give information related to the use of contraceptives or reproductive activity to private entities like menstruapps. We simply use these cases to provide context of the broader legal landscape rather than a comprehensive list. Furthermore, these cases concern state power and surveillance, and while there is a robust literature and case law there, what is less analyzed and well developed in the legal literature involves questions of surveillance from private businesses and surveillance to which the user consents via a privacy policy. What makes these cases important is that they lie at the intersection of privacy and reproductive rights and provide useful context for understanding the current state of privacy surrounding products that can aid with reproductive autonomy and decision making.

Privacy and femtech/menstruapps

Changes in technology, particularly the rise of the internet and social media platforms, have complicated matters of privacy. What does the "right to be left alone" even mean when people are sharing every intimate detail about their lives with private for-profit businesses? Concerns about digital privacy came relatively early on in the age of internet (e.g. Kang 1998; Schwartz 1999) and a literature far too extensive to fully document here has developed. However, there are several key themes in this literature that are worth exploring the current context.

Evolution of menstruapps – purpose and evaluations

In 2009, Piraye Yurttas Beim, a molecular biologist and founder of Celmatix, a biotech startup focused on women's health, was in search of funding for her startup that would combine the power of big data with genetic testing to understand and treat infertility (Altman 2019). However, Beim struggled to find investors, having two strikes against her: being a woman in the male dominated tech world and the fact that she was catering to a niche market. Collectively, the menstruapps that are now supported by this supposedly niche market were valued at $1 billion in 2018 and are estimated to be worth $50 billion by

2025 (Shipp and Blasco 2020). Founded in 2013 by PayPal's Max Levchin and four other men, one menstruapp called Glow, had no such problems attracting funding, sweeping in $23 million in its first year (Tiffany 2018). What caused this pivot in the tech industry? Did it somehow become pro-women?

Most would agree that the answer is a resounding no. Even after the success of Glow, Apple Health, released in 2014, faced massive criticism for its omission of any sort of capability to track menstruation. Once the applications began to proliferate, so did the scholarship on their dangers. Some centered on the functionality of the applications. Moglia et al. (2016, 1157) conducted a systematic evaluation of menstrual cycle tracking applications and conclude that most smartphone applications are "inaccurate, contain misleading health information, or do not function." Shipp and Blasco (2020, 503) review the privacy policies of 30 Android menstruapps and find that while basic personal data is generally treated appropriately by most applications, reproductive data is not covered by the privacy policies and that the applications have "a significant amount of issues that could lead to serious consequences given the data they handle consists of information like sexual orientation, menstruation, and pregnancy." Further, others raise concerns about assumptions made by these applications, such as the fact that many treat pregnancy, rather than pregnancy prevention, as the goal. Eighty percent of the applications in the Moglia et al. (2016) sample contained information for conception while only 50% contained information about contraception. As Tiffany (2018) wrote for *Vox*, these applications weren't, " ... designed for me ... they're designed for marketers, men, for hypothetical unborn children," but *not* for women.

Reproductive surveillance in the age of surveillance capitalism

Other scholarship centers upon reproductive surveillance. Goodwin (2020) introduces the idea of "hospital snitches," which adds the element of "trust" to the question of surveillance. Specifically, these are trusted individuals in a hospital setting that "snitch" on their patients to police or hospital legal teams for seeking to terminate a pregnancy or engaging in behavior that would endanger their fetus. This surveillance, conducted in what is believed to be a safe and confidential setting, parallels the use of menstruapps in that individuals are turning to a resource for assistance only to have the information provided to that resource used against them. We are told to trust doctors and nurses with information about our health and health care behaviors, yet they sometimes inform the police of this behavior, such as terminating a pregnancy. This highlights an important element of the surveillance conversation. Whereas traditionally it is law enforcement conducting the surveillance, when surveillance is being conducted by a third-party (i.e., the doctors and nurses or the menstruapp companies) the risks are obscured because the individual expects to be safe or protected. This may also explain some of the worry following the *Dobb's* decision and the calls to delete menstruapps; it was not until then that users realized the information they voluntarily gave up might endanger them.

Conti-Cook (2020) also describes how confiding in medical staff can result in criminal prosecution, but adds an additional layer. She highlights how an individual's internet search history related to their reproductive health, such as searches for abortion clinics or medication, could be used as additional evidence in their prosecution. While the Health Insurance Portability and Accountability Act of 1996 (HIPPA) protects a person's sensitive health information from being disclosed by certain entities, many people mistakenly believe this is a blanket protection (Germain 2021, 2022; Kavi 2021). Just as HIPPA does not prevent companies like Google from handing over internet searches for abortion providers and medication to law enforcement, it does not prevent companies like Glow (a menstruapp company) from handing over user data to them either. Confusingly, while this communication could be protected in the context of a conversation one has with their doctor, the sharing of that information with menstruapp does not receive the same protection (Roberts 2022). This would seem to make the illusion of protection provided by the privacy policies of menstruapps an even more serious matter; however, even if they are aware, what can users do about it? According to Turow et al. (2023), most people think nothing. They find that while Americans say they care about their privacy and believe

that they are likely harmed by what is happening with their online data, they don't actually understand what the companies can or cannot do with it, and think they are helpless to control it anyway.

This emphasizes how the use of technology adds additional dangers for women. Eveleth (2014) quotes sociologist Deborah Lupton, "When you look at these types of apps, they're completely about the surveillance of pregnant women, making them ever more responsible and vigilant about their bodies for the sake of the fetus." Levy (2015), coining the term "intimate surveillance" warned of the influence these technologies could have on intimate relationships, arguing that they have the potential to facilitate heightened surveillance and control, even abuse. Citron (2022), through detailed accounts of violations of intimate privacy, illustrates the reality of what Levy had warned. She emphasizes the importance of protecting personal autonomy through strengthened privacy measures, and advocates for a collective effort to safeguard individual privacy.

Following the *Dobbs* leak, massive alarms went up in mainstream media and on social media platforms about the dangers presented by menstruapps, with recommendations to just delete them (Brody 2022; Tschinkel 2022). Kalish (2022), writing for *Mother Jones*, points to a study by Koepke et al. (2020) on "mass extraction" or the ability of law enforcement to search mobile phones and argues that it's an obvious extension for law enforcement to turn to menstruapps in order to prosecute illegal abortions. Kalish goes on to quote a digital security expert who said: "We've decided in America that abortions are a consumer good and not a right," eerily echoing Rosenberg's (1991) quote of Janice Goodman referenced above. Zuboff (2019) describes "surveillance capitalism," as an economic system in which corporations extract and monetize personal data from individuals, using it to predict and influence their behavior for profit. This form of capitalism, she argues, transforms human experiences into valuable commodities, eroding privacy and reshaping power dynamics in the digital age. This project sits at the intersection of these competing questions regarding the influence of the courts, privacy, and reproductive rights, but adds the *Dobb's* decision and the legal uncertainty that it produced as the intervening variable. While we naively may have expected to see an impact of *Dobbs* in the privacy policies we analyzed, especially given the media attention, our analysis suggests that most applications were not responsive to the changing legal environment, or the new risk their users could face, based on the data they collected.

Methodology

We utilized AppMagic, a mobile market intelligence tool, to find the most downloaded menstruapps. AppMagic obtains data from Apple and Google mobile applications stores and mobile app publishers and uses it to estimate revenue and downloads for mobile applications.[5] We filtered for applications with the tag "Period Tracker," on the year 2022, and included "All stores." This returned a list of the 46 most downloaded applications worldwide.[6] After removing applications not available in English, and one that was not actually a cycle tracking application, our sample includes 36 applications under 25 different parent companies covered by 23 unique privacy policy names. Table 1 displays each policy name, their parent company, the applications covered by the policy, and the location of the headquarters of the parent company. Some parent companies covered multiple applications, and some applications had multiple parent companies, so the ultimate unit of analysis is the privacy policy which we will refer to by the "policy name" throughout the remainder of the article.[7]

We aimed to collect each update to these privacy policies beginning with the last update prior to January 1, 2021, as this would be well prior to the Court granting cert on *Dobbs*, and continuing through November 7, 2022, which is just after the 2022 midterm elections. Not all the companies originally examined had updates available prior to January 1, 2021, so in those instances, we collected the earliest privacy policy available online. We approached the process of collecting the privacy policies in one of three ways. First, the websites of Flo and Glow provided archives of their prior privacy policies. For companies that did not provide an archive of past policies, we made use of the WayBackMachine, which archives URLs at different points in time. Using the URL for the current privacy policy, we collected all of the snapshots available on the WayBackMachine. From here the data

Table 1. Parent Companies of Applications.

Policy Name	Parent Company	Application Name	HQ Location
28 Wellness	28 Welness, LLC	28 Period Tracker & Fitness	US
Clover	Wachanga	Period & Cycle Tracker – Clover	Cyprus
Clue		Clue Period Tracker & Calendar	Germany
	BioWink GmbH		
	Clue Period Tracker by BioWink		
Femia	Magicfit Limited	Ovulation & Fertility – Femia	Cyprus
Femometer		Femometer Fertility Tracker	China
	Bongmi Global Group		
	Femometer Limited		
Flo	Flo Health United UK Limited	Flo Period and Pregnancy Tracker	UK
Glow	Glow		US
		Glow: Fertility, Ovulation App	
		Period Tracker – Eve	
GP Apps	GP Apps		US
		Period Tracker by GP Apps	
		Period Tracker HD	
		Period Tracker Deluxe	
Heena	Heena Health – Pregnancy Tips	Heena Health	India
Leap	Leap Fitness Group		Australia
		Period Calendar Period Tracker	
		Period Tracker Period Calendar	
		Ovulation & Period Tracker	
		Period Calendar Pro	
MeetYou	Meet you	MeetYou – Period Tracker	China
Menstrual Cycle Tracker	Anastasia Kovba	Menstrual Cycle Tracker[1]	US
		Fertility & Period Tracker	
		Fertility and Period Tracker	
		Menstrual Periods Tracker	
		Fertility Tracker for Women	
My Calendar	SimpleInnovation		US
		My Calendar – Period Tracker	
		Period Tracker & Diary	
		Cycle Tracker: Period Calendar	
NaturalCycles	NaturalCycles Nordic AB	Natural Cycles App	Sweden
Ovulation Calendar	Arbor Ltd	Ovulation Calendar and Fertility	Czech Republic
PepApp	Pepapp Teknoloji Anonim S¸irketi	PepApp	Turkey
Period Tracker	Maple Labs Co., Ltd.	Period Tracker – Cycle Tracker	Vietnam
PinkBird	Test speed internet & Net meter	Period tracker by PinkBird	China
PregTest&Tracker	Lihuayi	Pregnancy Test & Tracker	China
Spot On	Planned Parenthood Federation of America, Inc.	Spot On Period Tracker	US
Stardust	Stardust App, LLC	Stardust Period Tracker	US
WoCute	MQJC Technology	WoCute – Period Calendar	Singapore
WomanLog	Pro Active App SIA		Latvia
		WomanLog Calendar	
		WomanLog Pro Calendar	

[1]Original app no longer available.

collection took two different paths. Some companies provided "effective as of . . . " markers. This allowed us to eliminate some of the snapshots and retain only each new version of the policy. However, other companies did not provide this marker, so we were forced to treat each snapshot as a different policy for the next step in our analysis. Table 2 displays the policy names, the number of data points we were able to obtain for each, whether there were substantive changes made to their privacy policies, and whether the company released a statement on the *Dobbs* decision.

Our first important finding is that of the 23 policies we started with, eight of them either did not update their privacy policy during the timeframe or we were unable to identify any earlier versions of their privacy policy. For the 15 companies that did have multiple data points, the next process involved identifying specific changes from one policy to the next. We used an online tool called Diffchecker[8] that takes two files as input and generate a side-by-side comparison of each line, highlighting any differences. We used this tool to generate comparisons of each chronologically sequential policy for all

Table 2. Policy Details.

Policy Name	No. Data Points	No. Unique Policies	Substantive Changes	Statement on *Dobbs*
28Wellness[1]	1	1	No	No
Clover	13	1	No	No
Clue	7	7	Yes	Yes
Femia	1	1	No	No
Femometer	4	1	No	No
Flo	4	4	Yes	Yes
Glow	4	4	Yes	No
GP Apps	27	1	No	Yes
Heena	1	1	No	No
Leap	7	4	No	No
MeetYou	2	1	No	No
Menstrual Cycle Tracker	7	1	No	No
My Calendar	1	1	No	No
NaturalCycles	5	5	Yes	No
Ovulation Calendar	1	1	No	No
PepApp	1	1	No	No
Period Tracker	1	1	No	No
PinkBird	2	1	No	No
PregTest&Tracker	3	3	No	No
Spot On	2	2	Yes	Yes
Stardust	2	2	Yes	Yes
WoCute	1	1	No	No
WomanLog	3	3	Yes	Yes

[1]New company as of late 2022 so September 7, 2022 was first privacy policy.

companies that had multiple data points. Six of the companies that had multiple snapshots but did not provide the effective date marker, ended up having no changes across the snap shots.

For the remaining nine companies that did have changes, we built a dataset that included company name, type of change (i.e.: addition, deletion, or modification), date of each policy, changes to the policy text, whether it was a substantive change, and any notes the researchers thought were relevant. Two of the companies had only minor changes such as changes in e-mail addresses, leaving only seven companies with substantive changes to analyze. Table 3 displays these companies and the dates of their various policies. Due to the vast differences across these privacy policies and the language that they used, the analysis is qualitative in nature. To understand the significance of the type of change, the analysis needed to not only focus on the change in context and how that change fit within that individual privacy policy, but also how it compared to those that came before or afterward as well as in relation to the broader pool of policies analyzed.

Analysis

The first main question is whether the privacy policies we analyzed respond to the changing landscape regarding reproductive rights. The complicated answer to this question is a qualified, kind of. Of the 15 companies that had multiple data points to analyze, nine of them had policies before the *Dobbs* decision was released, either the official release or the leaked version, and then updated them at some time afterward. However, it is not clear that these changes were necessarily in response to *Dobbs* and the changing legal landscape, or if they were unrelated.

Substantive changes

While some of the companies included here, such as Glow, Stardust, and Clue, made significant changes to their privacy policies during this period, this was not universal. Femia, Heena, My Calendar, Ovulation Calendar, PepApp, Period Tracker, and WoCute did not have any updates available for their privacy policies before or after *Dobbs*. Using the WayBackMachine we collected 27 different snapshots in time of GP Apps' policy, 13 of Clover's privacy policy, seven of Menstrual

Table 3. Policy Dates.

Policy Name	Policy Sequence	Date
Clue	Original	December 1, 2020
	Change 1	February 23, 2021
	Change 2	August 182,021
	Change 3	October 21, 2021
	Change 4	January 17, 2022
	Change 5	March 14, 2022
	Change 6	May 25, 2022
Flo	Original	October 24, 2020
	Change 1	November 5, 2021
	Change 2	December 14, 2021
	Change 3	September 14, 2022
Glow	Original	December 17, 2020
	Change 1	November 21, 2021
	Change 2	September 5, 2022
	Change 3	October 25, 2022
Natural Cycles	Original	August 11, 2019
	Change 1	January 4, 2021
	Change 2	November 24, 2021
	Change 3	June 30, 2022
	Change 4	March 6, 2023
SpotOn	Original	April 10, 2018
	Change 1	June 7, 2021
Stardust	Original	June 26, 2022
	Change 1	October 19, 2022
WomanLog	Original	November 19, 2019
	Change 1	May 6, 2021
	Change 2	April 22, 2022

Cycle Tracker, four for Femometer, and two for each MeetYou and PinkBird dating from October 14, 2020, through November 3, 2022. Possibly more troubling, two of the applications we examined; PepApp and Period Tracker Cycle Tracker, had privacy policies that were last updated in 2018 and 2019 respectively.

The lack of changes here is significant given the dramatic changes to the landscape of reproductive rights between October 2020 and the fall of 2022. While it is possible that the companies felt that their privacy policies were sufficiently protective and therefore did not need to be changed, we are skeptical of reaching that conclusion. Even if a privacy policy had been written in such a way that it provided an iron clad protection of the user's privacy prior to *Dobbs*, it is unlikely it could continue to do so amidst all the changes during this period. Contrastingly, Spot On, an application developed by Planned Parenthood, updated their privacy policy on June 7, 2021. While this is more than a year before the Dobb's decision, it is after both the granting of certiorari on *Dobbs* and the passage of SB8 in Texas.[9] Other applications like WomanLog, last updated their privacy policy on April 2, 2022, a month before the leaked version of the *Dobbs* decision. Figure 1 shows a timeline of policy changes for the seven companies that had them, and notable court action.

On the other hand, some applications did appear to respond to the Dobb's decision. For example, Stardust explicitly recognizes that the data they collect poses a unique risk in the current political climate. We analyze Stardust in more detail below given the uniqueness of their privacy policy. Glow also seemingly responded to the changing legal landscape. On September 5, 2022, Glow updated their November 11, 2021 policy, by adding in a passage about being able to request to have your data deleted. While they seem to be responding to changing data protection laws in California, The California Consumer Privacy Act (CCPA),[10] they do go on to add that even users outside of California can request to have their data deleted and that they will do so within 30 days. Glow refined this in their next privacy policy update on October 25, 2022, by saying users can delete data from the Glow servers but retain it on their phone and clarify that this includes "Key Health Data." This change, allowing users

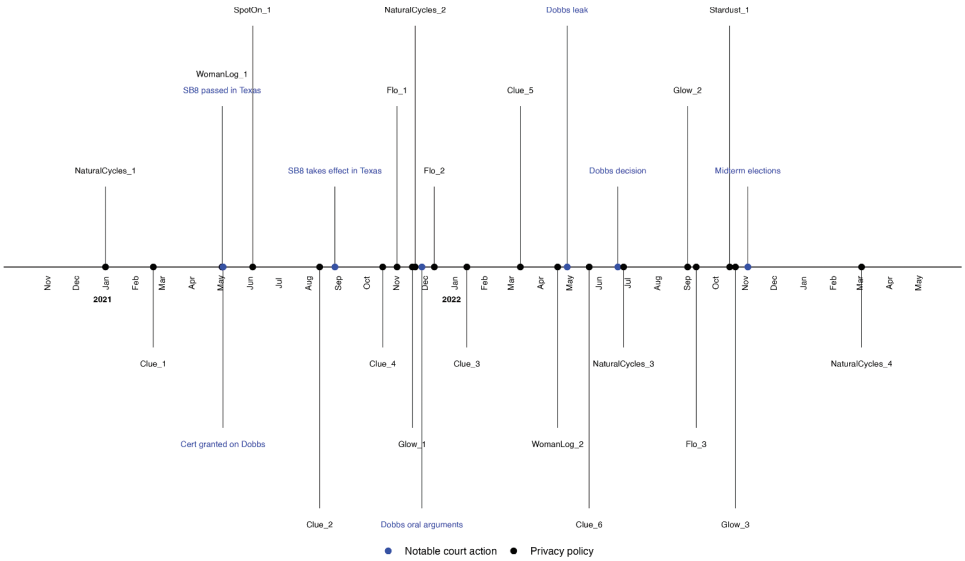


Figure 1. Timeline of Policy Changes and Notable Court Action.

to delete their data from servers but retain it on their phone, may be seen an attempt to allow users to continue using the application while also retaining more control over their own data. We discuss later that this may simply be a form of security theater, rather than an effort to meaningfully protect users.

Flo was another application that made changes before and after the Dobb's decision. For example, updating their December 14, 2021 policy on September 14, 2022, Flo explained that they had added an anonymous mode. This mode allows users to access and create an account without the identifiable requirements a normal account requires, such as "email, name, and technical identifiers." Additionally, they explain how previous identifiable accounts cannot be linked to a new anonymous account, and that users can request that their previous account data be deleted from their servers. While the feature was already underway as of the company's June 30, 2022 press release, Flo claimed that, "the development has been accelerated in the wake of the US Supreme Court's ruling to overturn the landmark case *Roe v Wade*."[11]

However, a complaint filed by the Federal Trade Commission (FTC) in 2020 alleged that Flo had been misrepresenting its data practices to users, disclosing health data from millions of users to various third parties, and had violated both the EU-US Privacy Shield and Swiss-US Privacy Shield. Flo agreed to a settlement in January 2021 which requires them to, "among other things, obtain an independent review of its privacy policies and get app users' consent before sharing their health information" (Federal Trade Commission 2021). In a press release on May 23, 2022, Flo addressed the issue stating that the settlement was not an admission of wrong doing, and that they had successfully completed the independent privacy audit which "did not identify any material gaps or weaknesses" in their policy.[12] Still, the timing makes it unclear whether the anonymous mode was a response to the audit findings, or to the changing legal landscape surrounding abortion.

Clue also presents an interesting evolution. From their August 6, 2021 policy to the next update on October 21, 2021, Clue added the following passage to their privacy policy,

> [w]ith regard specifically to the United States, the information we and our sub-processors maintain is unlikely to be the subject of inquiry by a public authority in the US that would invoke such laws that may compel a sub-processor to hand over personal information. The risk of such disclosure, however, cannot be eliminated.

and second about legal requests for the data on its users,

> We may disclose information we collect, including your personal data, when we in good faith believe that disclosure is required to comply with the law, a court order, or a subpoena. We may also disclose your personal data to prevent or investigate a possible crime, such as fraud or identity theft.

These modifications occurred following the passage of Texas SB8 and the legal uncertainty that it created. Interestingly, the statement about disclosing data following a legal request, which was added in the October 2021 update was then removed from the policy in an update on May 25, 2022.

Despite not updating after the *Dobbs* decision, WomanLog does make an interesting modification to their November 19, 2019 policy when they updated it on May 6, 2021. First, they provide information about where the server for the application's data is located. Given the varied nature of global data protection and privacy laws, the location of the server could be valuable information to users. Second, they added a section to the policy on how one could delete their account along with any user data stored via the application. However, in a slight difference from other applications WomanLog does not specify how long it will take for this deletion to occur, something other applications that we analyzed did specify.

In all, there is some response to the changing legal landscape. But those responses do not always appear to be in response specifically to *Dobbs*. As mentioned above, nine of the companies analyzed had changes that we could identify before and/or after the release of the decision. However, of those, we do not see a significant number of independent changes over this time. Rather, the changes documented coincide with many other legal changes unrelated to *Dobbs*. For example, the WomanLog and Clue changes follow the enactment of Texas's SB8, Glow appears to be responding to a change in data privacy laws in California, and Flo may be responding to bad press surrounding the FTC complaint.

Identifying the reason for these changes is a challenge. Without their explicit mention of why something changed, we are left drawing inferences given the timing of the changes, what was changed in the privacy policy, and the changes in the world. That being said, at the outset we expected there to be clearer responses to the legal changes ushered in over the time frame analyzed. Given the risk to users that the data these companies collected and particularly the media attention that risk received (Garamvolgyi 2022; Morrison 2022), it was surprising to not see more robust changes. While the difference between terms and conditions and privacy policies is supposedly that terms and conditions are to protect the providers while privacy policies are to protect the users, we would argue that this provides evidence to the contrary, and that instead the privacy policies are also there to protect the companies. This is not a novel claim, Turow et al. (2023, 4) summarize Schwartz's (1999) argument that privacy policies are "generally meaningless since they are often ignored by individuals, written in vague legalistic language, and fail to present meaningful opportunities for individual choice." In light of this, we turn now to some broader evaluations of the privacy policies in our sample.

Broad evaluations

Beyond looking at the potential response to changes to the reproductive right's landscape, another element of this project was to analyze any other changes over the course of our data collection period, as well as the level of protection afforded to users in general. While we found some evidence of responsiveness, these other questions speak more broadly to the purpose of the policies. What motivates companies to make changes to their policies, and what, if any, real protections do they provide?

General commitments to privacy

In general, the privacy policies contained statements about a commitment to the privacy of users. For example, PinkBird's March 1, 2022 privacy policy opens with "We, Hangzhou AtlasV Technology Co., Ltd. [the parent company of PinkBird] and its affiliates, are committed to protecting your privacy. We limit the collection of your data. We only collect data that is required to maintain PinkBird." Spot On,

a tracker developed by Planned Parenthood,[13] has a much more detailed statement at the start of their June 7. 2021 privacy policy,

> Planned Parenthood Federation of America, Planned Parenthood Action Fund, and Planned Parenthood local organizations . . . respect and are committed to protecting the privacy of users of our websites, applications, and other online and electronic services. . . We want our Online Services to be safe and helpful, and to help make you aware of our data practices we drafted this Privacy Policy, which describes the ways in which Planned Parenthood uses, discloses, and collects information from or about you through www.plannedparenthood.org, www.plannedparenthoodaction.org, and all other Online Services that link to this policy. Please be aware that your use of the Online Services is not guaranteed to be anonymous, and Planned Parenthood may collect, use, and disclose information about your use of the Online Services as set forth in this Privacy Policy.

All of the policies expressed something similar to this. The reality is though, that this is not sufficient. There is a difference between stating a commitment to privacy for users and actually engaging in practices that protect user's privacy. It is therefore necessary to dig into the privacy policies in more detail.

Legal concerns

Sixteen of the 23 companies in the sample stated in their policies that they would comply with requests for data from either law enforcement or government entities.[14] However, of these 16, four included some sort of qualification that made it clear they would go to at least some length to limit the data provided as much as possible only sharing what was explicitly required. For example, 28 Wellness states: "To comply with any court order, law, or legal process, including as required to respond to any government or regulatory request, but only to the extent legally required. We will never voluntarily provide your personal information to the government." It is worth noting that, while they do include caveat their policy only applies to their own practices and not those of their affiliates that link to their website or application, they state that they do not share users' personal information with third parties for promotional purposes and they do not use information they collect to deliver targeted advertisements to the user.

Another company to qualify their compliance with law enforcement requests was Natural Cycles. The original verbiage in their policy states that they will share data "if we reasonably believe it is necessary to comply with a legal or regulatory obligation. However, in their March 2022 update, this changes to:

> Natural cycles will provide personally identifying data in response to a third-party inquiry only if required by a valid legal process but will take all possible steps to keep your data private. Natural Cycles will contest the disclosure of your personal data in response to a third-party inquiry to the extent that a reasonable ground for objection exists. Natural cycles will provide you with prompt prior notice of such a request, to the extent legally permitted, so that an order for relief may be requests. If Natural cycles determines that such a disclosure is legally required, then it will seek a confidentiality designation protecting the disclosure, and will only disclose he portion necessary and at the required time.

While this update was a bit outside of our collection window, we felt it was important to include in our analysis because their June 2022 policy added the statement: "Please note: we are currently reviewing our privacy policy to better protect our users and their data in today's world. We will be updating it as more information becomes available." While this note does not explicitly reference *Dobb*s or reproductive rights, we believe the content of the change clearly suggests that is what is meant.

Stardust took what seems to be an even more explicitly defiant approach in their language. In the October 19, 2022 update to their privacy policy Stardust added the following:

> What happens if law enforcement sends us a subpoena for your data: We cannot prevent the government from issuing a subpoena. However, in such a case we would not be able to produce your period data because we cannot connect it to your login information. We do not know which data set belongs to which person.

Stardust expressed in their privacy policy that they were particularly aware of the political climate and the threats posed by the changing landscape around reproductive rights. This language also reflects

a choice by the companies. Stardust makes it clear that they are not in the business of data collection and sale adding in their October 19, 2022, update the following two passages: "Unlike most of our competitors, we have never sold data in the past and never will. It is neither our business model nor our philosophy to do so" and,

> We will not sell your data. Full stop. This includes everything from email address to pregnancy status to location. Instead of selling data, which is how some period trackers earn money, we will one day charge for paid features within the app. We believe this is a healthy way to make sure our incentives remain aligned with those of our users.

If we accept the language at face value from Stardust and other privacy policies analyzed, we can see the tension inherent in this data economy. Stardust has forsaken the surveillance capitalism model of revenue; while this allows them to avoid (in theory) having to hand over specific user data since "[w]e do not know which data set belongs to which person" they are also losing out on this source of revenue.

The implication here is that companies where user profiles and their health data are linked are able to capitalize upon the sale of this data, but also run the risk of being subpoenaed and forced to hand over the data they have collected. Though this has not happened yet, this places companies in a particularly difficult position regarding privacy commitments, something to which many of them at least express a surface level commitment. By collecting this data, they are putting their users inherently at risk. This is heightened by two important factors for users within the United States,[15] the uncertain landscape of reproductive rights in the post *Dobbs* era and the weak, if not non-existent, privacy protections individuals are afforded regarding their data. However, not collecting this data in an identifiable or linked manner would challenge the financial viability of many of these applications, especially those that do not charge a fee for using the application.[16] Therefore, in the wake of *Dobbs*, companies are forced to decide between protecting the privacy interests of their users and their own bottom line. It seems impossible given the current political climate and legal standards to respect the privacy interests of users and participate in the data economy.

Stardust

Of all the companies analyzed, Stardust was the most open about responding to the current political and legal climate regarding threats to reproductive rights. In their October 19, 2022, updated privacy policy, they added the following at the beginning of the document,

> Stardust is an astrological period tracker owned and operated by a team of three women based in New York City. Given the current political climate, we have taken rigorous measures to protect users, especially those in states where abortion is being criminalized. We believe all period trackers should stringently protect the privacy of users —and be transparent about exactly how they do so.

First, the mention that this is a company "owned and operated by a team of three women" is an important signifier. A criticism of the tech industry broadly but especially salient in the recent discussion about period tracking applications is that this is an overwhelmingly male dominated field. Stardust was not the only one to highlight that they were a company owned by women, but this mention is significant in light of the rest of their privacy policy.

In addition to the previous discussion about the sale of data, Stardust goes out of its way to discuss ways to further protect the privacy of users. For example, while they do not tell users to use fake names, they do say in the updated policy regarding usernames that "[I]t doesn't have to be your actual name! You can use any username you'd like." The language here taken in conjunction with the earlier discussion of how they store data separately would strongly suggest that Stardust does not desire to sell user data because they tell users how to diminish the usefulness of that data. Further, Stardust recognizes that not only is the data they have a potential danger to the user, but also that the data on a user's phone is a danger as well. Stardust is unique in the inclusion of the following in their privacy policy, speaking directly to this reality:

> If law enforcement obtains your phone and forces you to unlock it through biometrics, we cannot protect you yet. We are building a way to lock the app with a PIN and this will be ready in the coming months. If you live in a place where you are especially vulnerable, we recommend you track your period in a paper journal and store it in a secure place.

Not only does Stardust express a commitment to privacy and takes steps to deidentify user data, but they actually advise users who are particularly "vulnerable" to use pen and paper instead of the application. In the surveillance capitalism landscape, this suggestion stands out.

Third parties and data capitalism

A major issue regarding privacy is that the data collected by the application is that not limited to just that application. Instead, applications make use of several third-party companies to accomplish many tasks related to the functioning of the application. This can include things like feature testing, data storage, or enabling other features in the application. All of this means that the applications in question are sharing user data with these third-party processors. Many of the privacy policies recognize this and state that while they share data with these third parties, that data is in turn subject to the privacy policies of those third parties. Other privacy policies did state that they placed a limit on the ways in which third party providers could use the data, what data would be shared with them, or the form data shared with them would take (i.e., if it would be anonymized or not). This opens up a rabbit hole[17]; data flows between different companies and while privacy commitments may be relatively strong at one stage of that process, companies in other parts of the process may be less committed to those protections, thus creating a system where the weakest privacy policy in the chain is potentially the most important and dangerous to the user.

Clue, in its update on February 23, 2021, states that it does not work with "sub processors" who are in countries where the rule of law with respect to privacy is of concern. While Clue is not alone in this stance, the fact remains that many of their processors, sub-processors, and other vendors are located within the United States, who lacks robust, or clear, data privacy laws. Clue, who is headquartered in Germany, recognizes this tension and in the October 21, 2021 update acknowledges that sub-processors located outside the EU "including in particular the United States" may be compelled to turn over the data they collect. In this same update Clue felt that the data it and its sub-processors collected was unlikely to be sought by a public authority in the United States stating that:

> With regard specifically to the United States, the information we and our sub-processors maintain is unlikely to be the subject of inquiry by a public authority in the US that would invoke such laws that may compel a sub-processor to hand over personal information. The risk of such disclosure, however, cannot be eliminated.

A major concern in the post-*Dobbs'* world is how the personal health data collected by these applications is shared and sold by third parties. Particularly around pregnancy and reproductive healthcare, this information is not only valuable in the traditional "informational capitalism" (Cohen 2019) or "surveillance capitalism" (Zuboff 2019) sense, but also now may be valuable, ideologically, criminally, and/or financially, to those seeking to target pregnant people under laws such as SB8, Texas' "Bounty Hunter" law.

Of the companies analyzed, many were transparent about which third party applications are used and for what purposes. Others simply stated that their application used these vendors, such as Menstrual Cycle Tracker who stated, "We may share non-personal information with third parties who provide services such as information processing. These companies are obligated to protect the information." Stardust provides an example of a more detailed discussion of these third-party vendors explaining their relationship with Mixpanel, a "user analytics" company in very clear terms:

> We use Mixpanel to help with user analytics, so we can make better product decisions. For example, is anyone actually using this new button we designed or should we get rid of it? In this case (and all cases), we do not know who is actually tapping the button, because we save personal identifiable information in a different place from all other data.

Clue makes mention of Google Analytics and provides a link to get more information about their services. However, Clue's policy regarding what is shared with these third-party vendors is unclear. In January of 2022, Clue had the following to say about third parties and how they used data generated through the Clue application:

> But we are careful to only let them process usage data and minimal personal data on Clue's behalf, not data relating to your menstrual cycle or other health data. To be clear, these third party [sic] services are not permitted to use the data for any other purpose than to help us run Clue.

In March of that same year, this section of the privacy policy was shortened to remove the first sentence and just say, "To be clear, these third party [sic] services are not permitted to use the data for any other purpose than to help us run Clue." This same policy also went on to clarify about the types of data necessary for the application to function:

> Health and sensitive data We process health data and sensitive data that you choose to track in the Clue app to provide our service to you. Such health data may include include [sic] your cycle information (e.g., period length, pain, or spotting) and depending on the data you provide, it may also contain information about your general health (e.g., weight, body temperature, hair quality, and if/how you engage in sexual intercourse) This data is necessary for Clue to deliver the services you use. We only process the data you provide to us by tracking it in the Clue app. In order to personalize certain in-app messages we send to you as part of our Clue service, for example, individual insights, reminders or suggestions regarding information you might find useful in your lifestage [sic], we also process health data that you choose to track in the app.

It appears based on these two passages that the third-party vendors very well may have access to the very type of information that would put a pregnant person at legal (civil or criminal) risk. While Clue may express a commitment to privacy, sharing user data with the broader information capitalist system could possibly endanger the user. This also highlights the way in which user data spreads throughout this ecosystem, the data collection through one application is shared with other companies who might be willing to sell or share that data with other brokers. It appears that when it comes to protecting users' personal information in this information capitalist economy, "the only winning move is not to play" (Badham 1983).

Clue, who was particularly active in updating their privacy policy, six times over the timeframe, specified who they shared data with and what type of data. In a substantial update on October 21, 2021, Clue refines their language around what data is collected, shared, and to whom. They specify that while they do share data with third party providers, that "sensitive health data" is not shared with the ad network. Further, that it stores profile data and cycle tracking data separately, in this section they changed the language from "this allows us to ensure the highest possible level of privacy for your cycle information" to instead say "this allows us to ensure an increased level of privacy for your cycle information." This shift in the language regarding privacy protections from "highest possible" to "increased level" would suggest a diminished commitment to privacy protections.

Clover, who did not change their privacy policy between November 24, 2020, and October 4, 2022, makes no bones about their use of personal data and how it is shared or used. In their discussion of working with third party applications, the policy states "These parties are contractually prohibited from using your personally identifiable information for any purpose other than for the purpose Wachanga [the parent company/developer for Clover] specifies." Just above this in the privacy policy, the list of what they can use your personal information for is quite expansive,

> to verify your identity . . . to personalize your experience when you use our Services. You can personalize your experience by adding health data into your profile, completing assessments, or using other services we offer. We will use this data to personalize Services, track your symptoms, assess your health, and display articles of interest to you . . . to link or combine with information we get from others (except data from Apple HealthKit, Core Motion Framework, and Google Fit) or (and) from you to help understand your needs and provide you with better service (to use in the training of neural networks, artificial intelligence, as well as for any other automated decision-making processing) . . . for scientific and academic research purposes; and for any other purposes disclosed to you at the time, we collect Personal Data or any other purposes indicated in this Privacy Policy.

Equally interesting is that in the Clover policy they have a statement about what happens if Wachanga is bought or sold, something that in the tech industry seems to be a common occurrence,

> In the event that all or substantially all of Wachanga's stock and/or all or substantially all assets are transferred or sold to another entity, Wachanga may transfer personally identifiable information to the acquiring entity. If, as a result of such a business transition, your personally identifiable information will be used in a materially different manner than as described herein, you will be given choice consistent with our policy regarding notification of changes.

This was a unique addition to the privacy policy, and something not found in any other company's policy which on its own raises important questions. However, while the statement says that "you will be given a choice. . ." if the company is sold and the data collection/usage will change it does not say what that choice would be. Presumably a user could decide to stop using the application, but that does not clarify what happens to that user's data that was previously collected and if it will be deleted or not.

Menstrual Cycle Tracker provides an interesting example. While Menstrual Cycle Tracker did not update their privacy policy between October 14, 2020, and October 6, 2022, their privacy policy does state that they "don't collect any personal information" and they define personal information as: "Personal information is data that can be used to identify or contact a single person." They also add that they do not *use* any of your personal information. Setting aside the seeming contradiction between the collect and use parts of the policy, something that could be attributed to translations and language differences since according to the GooglePlay Store page for the application it supports 67 languages,[18] this privacy policy is still vague in terms of the data collected and how it may be used.

While this application claims to not collect personal information and says "[w]e take the security of the personal information very seriously" the brevity of this policy, 414 words,[19] leaves a great deal of ambiguity. First, there is no discussion of the European Union's General Data Protection Regulation (EU GDPR), something many of the other applications discussed (six of the 12, to varying degrees, discussed or mentioned the EU GDPR). Second, the application states that "[a]ll the information you provide may be transferred or accessed by entities around the world depending on the actual location of their servers." However, it is unclear what countries are storing this data. This is important because the data protection laws vary across the globe (Citron 2022). Finally, returning to the issue of personal information, the privacy policy provides a vague definition but does not specify what information is collected that they deem to be unidentifiable. There is also the problem that "deidentified" data is hardly ever truly anonymized (Ohm 2010). Users who care about the privacy of their data need to have information to make an informed decision. While Menstrual Cycle Tracker may protect privacy, equally, more, or less than any other application, their policy does not provide users with the information one might consider necessary to make that decision for themselves.

Data deletion

All but three of the companies we examined discussed being able to request having data deleted. For example, in the October 25, 2022 update to Glow, the company explains the process for deleting data from their servers and from a device, stating this would be accomplished in 30 days. Stardust again goes stands out when it comes to data deletion, "You can delete your data at any time. Your data, your choice. To erase your data, simply hit the delete button within your profile. Within minutes your data will be gone permanently." While deleting data is common, the language here suggests that it can be deleted "within minutes" and is permanently gone.

Other applications are less open to deleting data. Clover states that it will delete the data of anyone under 13, or 16, depending on the location that it finds to be using its product. Given the protections of the EU GDPR, the application is limited in the EU in its use to those over 16, so their policy states, "If you are aware of anyone younger than 16 using the App, please contact us at team@wachanga.com and we will take steps to delete such information and (or) delete their account." In the US, Clover references the Children's Online Privacy Protection Act, and that parents or guardians can request to have the data of anyone under 13 deleted. Other users, it seems, are unable to have their data

deleted. Menstrual Cycle Tracker simply states "[t]o ask if we have any of your personal information you may contact us through one of the options provided at the bottom of this page," so it does not even give users the option of deleting the data collected. However, if they learn that they have collected data from someone under 13 they will delete that data "as soon as possible."

PinkBird is unique with their inclusion of a data retention section. This section of their privacy policy has three important parts. First, "[w]e retain your data when we have an ongoing legitimate business need to do so, such as providing you with a service you requested, or complying with applicable legal, tax, or accounting requirements." Second,

> when we have no ongoing legitimate business need to process your data, we will delete or anonymize it. If it is not possible to delete or anonymize your data (for example, because it has been stored in backup archives), then we will securely store it and isolate it from any further processing until deletion is possible.

Third and finally, they follow this with a right to be forgotten section which states,

> We will erase your data when: Your data is no longer necessary for the purpose which we originally collected or processed it for; You withdraw your consent to us holding your data, and we are relying on your consent as the lawful basis for holding on to your data; You object to our processing of your data, and there is no overriding legitimate interest for us to continue such processing; We are processing your data for direct marketing purposes and you object to that processing.

We can analyze the first two sections together. If we read them together this would mean that they will retain data indefinitely. If the data contained in their application may be used against a user, then this would create an ongoing legal need for them retain the data. The final section is also concerning. Specifically, the idea that they delete the data once it is no longer necessary to achieve the purpose it was obtained for is vague. Presumably the data is there to generate the application revenue, so that data will always have value by this logic. The fact that the application has carved out room for it to retain user data indefinitely is troubling and puts this application in a unique place compared to others, who state that users can delete their data even if there is a delay between the request and the actual deletion.

The time frame for when data would be deleted however varied. Some, like Flo, gave no time frame for when data would be deleted while others like Femometer said 15–45 days and Glow who said 30 days. Clue and MeetYou both specified that they would reach out to 3rd parties with whom data may have been shared. PinkBird, Clover, and Menstrual Cycle Tracker however were distinct in this regard. PinkBird and Clover imply that only EU residents, and specifically those under 16 for Clover, could request to have their data deleted. Menstrual Cycle Tracker however simply stated that those under 13 using the application could request to have their data deleted. Interestingly, Heena, Pregnancy Test and Tracker, and SpotOn were the only applications that did not make mention of having the option of deleting your data in some fashion.

This discussion of data deletion is more complicated than it would seem. The reality, currently, may be that by the real danger of the data isn't its existence on a server, but instead on an individual's phone. In one of the recent cases that has garnered media attention, an ex-husband is suing friends of his ex-wife for helping her to get an abortion. Specifically, he introduced into evidence in the complaint showing the messages between his ex-wife and the friends. However, those messages were not sourced by requesting them from the provider or network. Instead, he simply took pictures of her phone with his phone (Donegan 2023). This instance would suggest that the data contained on an application's server might not be the real danger to a user, and instead it is the data they have on their phone.

Of the applications analyzed most as we discussed had the option of allowing users to delete their data either off their phone and also the company's server, with various constraints. Glow discussed allowing users to delete data from the server and keep it on their phone, presenting this as the more secure and safe option, and empowering users by giving them more control. However as seen in the example from Texas above, it may be that storing data in exactly this way is the real danger. StarDust seems to recognize this danger, explaining how the data on their servers cannot be linked to an individual but if law enforcement gains access to a user's phone there is nothing they can do to protect

that data. These changes, some of which we documented previously, may be a form of security theater, giving users the sense of control and protection but not actually making them more secure or safe.

From the perspective of law enforcement, it also makes sense that if one wants to access information the easiest way to do so is going to be through a user's phone. Serving these companies, getting the data, combing through it to identify a particular user, and then making sense of that data is complicated and time consuming. Access to an individual's phone will be a simpler process, and is one that law enforcement already engages in.

Discussion

Following the *Dobbs* decision there was a great deal of discussion about the future of reproductive rights and in particular there was legitimate concern about how the data collected by menstruapps could be weaponized against users. The situation was novel and evolving in real time, but it was not unexpected nor was the danger that these applications posed unknown. In this regard, the lack of changes then to these privacy policies in particularly concerning. As states have moved to criminalize seeking an abortion, abortion providers, or aiding someone in getting an abortion, the data contained in these applications is increasingly valuable and dangerous. This is especially true if states follow the Texas "Bounty Hunter" model where individuals can receive a financial incentive for going after someone for seeking an abortion. By and large, while the fact that most of these applications have not taken stronger steps to protect their users is concerning, it is also not surprising.

As mentioned above, the only way to take user privacy and data security seriously is to not use that data. In reading through these policies only one application, Stardust, appears to store data in a way that does not put the user at risk, but they do so at what seems to be a financial cost. This also speaks to the idea suggested previously that the purpose of these policies is not to protect users but instead to protect the company. These applications are largely in the business of surveillance capitalism where user data is the product. What these policies articulate, is not how user data will be protected but instead how it will be collected, stored, used, shared, and/or generate profit. As a result, calling most of these privacy policies may be misleading, rather they more accurately could be called disclosure policies. Users are told how the data will be stored and then under what circumstances the data will be handed over, and to whom. Companies are protecting themselves from potential civil lawsuits and from state action through these privacy policies. Further, the policies analyzed present the ways in which the companies collect, use, share, and store user data as inevitable. However, the truth is that the surveillance capitalism model is not the only option. Companies can decide to protect user data in a more robust and meaningful way, but that also means they are not able to participate in the surveillance capitalist model.

There is also a twisted irony to all of this. Women of reproductive age are seeking out these apps for information about their health; information that is especially important as states seek to tighten access to reproductive healthcare. However, by turning to these apps users are leaving a digital trail of crumbs that those seeking to prosecute those users could find useful. As our analysis shows, the users, who are producing value for the company, are not receiving any real protection as the misleadingly labeled privacy policies generally seek to protect the company rather than the user. This lack of concern for women in tech is highlighted especially well by Citron (2022), companies are more than happy to profit off women but they are not willing to protect them or act in their interest. For example, she describes how the creators of Ovia Health (not included in our sample) marketed a paid version of its menstruapp "to insurers and employers as a way to reduce medical costs and shepherd new mothers' return to work" (Citron 2022, 34).

Fitting into this discussion is also the response to *Dobbs* specifically. Six of the apps we analyzed also put out statements about the decision, and unsurprisingly they were critical of it. For example, Clue on June 28, 2022, released a statement that began " At Clue, we strongly believe that the very personal decision to end a pregnancy should be made in the context of legal, regulated healthcare, without shame or fear of prosecution."[20] And Flo on June 24, 2022, said

"We will do everything in our power to protect the data and privacy of our users. We have comprehensive security measures in place and will never sell your personal data. We understand the deep responsibility we have to provide a safe and secure platform for you to use and want to remind you that you may delete your data at any time."[21–22] While it is encouraging to see two of the leading apps in this space respond to the decision and express a commitment to reproductive rights and recognize that they collect sensitive data, these are simply words. The privacy policies are instead where we see the rubber meet the road and we can see how corporate policy has changed. In that regard then the lack of responsiveness to *Dobbs* and the changing legal landscape is troubling. At best, we can view these companies as businesses that aim to make a profit, and to expect them to engage in behavior that could cost them financially may be too much to ask. Or, more cynically, we could view these statements as symbolic position taking: efforts to calm a worried user base in order to keep them as active users so they can continue to profit off of their data.

Speaking to the question of responsiveness, this data suggests that there is some responsiveness among private third-party actors to the decisions made by the U.S. Supreme Court. However, without specific mentions of why a policy was modified, the best we can do is attempt to triangulate the reason for that change based on the events in the world that we can observe. To this end, we see companies revising their privacy policies in areas that make sense following various legal changes given how the law has evolved. Future research should investigate this question further regarding the responsiveness of non-governmental actors, especially in cases like this where the third-party actor is not a party to the case, nor are they directly impacted by the decision but instead the influence could be viewed as more indirect.

Complicating matters further is the multi-national nature of these applications. Sixteen of the applications we analyzed are headquartered outside of the United States. Of the those, nine of them are further located outside of the European Union. This sets up a complicated set of legal questions regarding the protections of data, rights to have data deleted, and how state actors in specifically the United States can make requests that companies outside of the United States hand over user data. An additional complication will be how California's recent changes to their data privacy laws are implicated in this. Application data and particularly in the context of criminalization of abortion is an emerging area of law, and one that will continue to evolve at the speed of light.

Notes

1. For example, Idaho (Vestal 2023).
2. But see https://www.cnn.com/2023/09/23/us/nebraska-abortion-pill-jessica-burgess/index.html where Facebook handed over the messages between a mother and her teenage daughter that demonstrated the mother aided the daughter in getting a, now illegal, abortion. Based in part on the evidence in those messages, the mother was sentenced to two years in prison while the daughter was sentenced to 90 days.
3. For example, the website for Flo, one of the apps we analyzed, says "Understand your cycle and feel your best If you want to know more about your body and how your cycle can affect everything from your mood to your energy levels, tracking your periods and ovulation is a great place to start" (see https://flo.health/).
4. This is also complicated by location as Europe has more stringent protections of user data, especially when it comes to minors.
5. AppMagic estimates the accuracy of their daily numbers to be higher than 80%, and the accuracy of their monthly numbers to be higher than 90%. See https://appmagic.rocks/about.
6. Also see https://www.statista.com/statistics/1307702/top-period-tracker-apps-worldwide-by-downloads/. All applications in the Statista data were included in the AppMagic sample, and Statista cites AppMagic as one of the sources of their data.
7. See Appendix for an additional table displaying the policy name, application name, the application store in which it is available, and number of US and worldwide lifetime downloads.
8. See https://www.diffchecker.com/.
9. It is worth noting that Spot On had a lengthy and thorough privacy policy.
10. See https://oag.ca.gov/privacy/ccpa.
11. See https://flo.health/press-center/flo-launches-anonymous-mode.

12. See https://flo.health/press-center/flo-response-ftc-settlement-update.
13. We should also mention that the privacy policy from Spot On is encompassing of the larger Planned Parenthood website and their other online/digital services.
14. Not including Clue who added but then removed a statement of this type between updates.
15. We recognize that threats to reproductive rights are under threat globally, and other countries make the United States look liberal by comparison, but for our analysis we are limiting our discussion to the United States.
16. In instances where applications do not charge, the common refrain is that the application is not the product but instead that the user and their data are the product.
17. One that we do not fully explore in this article.
18. See https://www.anastasia-kovba.com/menstrual-calendars/.
19. For comparison, Clue's October 21st 2021 policy comes in at 7,216 words, StatDust's October 19th 2022 policy comes in at 3,527, and PinkBird's policy from April 2nd 2020 is 1,794 words.
20. See https://helloclue.com/articles/abortion/clue-s-response-to-roe-vs-wade.
21. See https://flo.health/flo-response-roe-v-wade.
22. As discussed previously, Flo also highlighted their "Anonymous Mode" in the same press release but the creation of that may have been in response to an FTC complaint, rather than being specifically motivated by the Dobb's decision.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Francis Marion University; Rutgers, The State University of New Jersey.

Notes on contributors

Katie Krumbhholz is a Ph.D. Candidate in Political Science at Rutgers, The State University of New Jersey - New Brunswick.

Alice Militaru is a Fulbright Fellow and earned a B.A. in French and a B.S. in Marketing in 2024 from Rutgers, The State University of New Jersey - New Brunswick.

Kyle J. Morgan is an Assistant Professor of Political Science at Francis Marion University. He earned his Ph.D. From Rutgers, The State University of New Jersey - New Brunswick in 2020. His research focuses broadly on American Public Law, Civil Liberties and Civil Rights, and Public Opinion.

ORCID

Katie Krumbholz http://orcid.org/0000-0002-2438-8025
Alice Militaru http://orcid.org/0009-0009-8232-0270
Kyle J. Morgan http://orcid.org/0000-0002-7920-4246

References

Altman, Anna. 2019. "Mommy and Data." *The New Republic*, January 14. https://newrepublic.com/article/152693/femtech-companies-alleviate-exploit-female-anxiety

Badham, John. 1983. *War Games*. MGM/UA Entertainment Company.

Brandeis, Louis D., and Samuel Warren. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5):193–220. doi:10.2307/1321160.

Brody, Ben. 2022. "Tech Companies Face a Legal Nightmare if Roe V. Wade is Overturned." *Protocol*, May 3. https://www.protocol.com/policy/abortion-tech-legal

Brown, Lisa Mclennan. 2004. "Feminist Theory and the Erosion of Women's Reproductive Rights." *Journal of Gender, Social Policy & the Law* 13 (1): 87–107.

Citron, Daniell Keats. 2022. *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age*. New York: W. W. Norton & Compnay.

Cohen, Julie E. 2019. *Between Truth and Power*. New York: Oxford University Press.

Collett, Teresa Stanton. 2003. "Fetal Pain Legislation: Is It Viable?" *Pepperdine Law Review* 30 (2): 161–84.
Conti-Cook, Cynthia. 2020. "Surveilling the Digital Abortion Diary." *University of Baltimore Law Review* 50 (1): 1–76.
Donegan, Moira. 2023. "They Helped Their Friend Get an Abortion. Now a Bitter Ex-Husband is Suing Them." *The Guardian*, April 15. https://www.theguardian.com/commentisfree/2023/apr/15/texas-abortion-bounty-hunter-law-friends-sued
Eveleth, Rose. 2014. "How Self-Tracking Apps Exclude Women." *The Atlantic*, December 15. https://www.theatlantic.com/technology/archive/2014/12/how-self-tracking-apps-exclude-women/383673/
Federal Trade Commission. 2021. "Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations That It Misled Consumers About the Disclosure of Their Health Data." *Press Release*, January 13. https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about
Flavin, Jeanne. 2010. *Our Bodies, Our Crimes: The Policing of Women's Reproduction in America*. New York: New York University Press.
Franklin, Charles H., and Liane C. Kosaki. 1989. "Republican Schoolmaster: The U.S. Supreme Court, Public Opinion, and Abortion." *American Political Science Review* 83 (3):751–71. doi:10.2307/1962059.
Garamvolgyi, Flora. 2022. "Why US Women are Deleting Their Period Tracking Apps." *The Guardian*, June 28. https://www.theguardian.com/world/2022/jun/28/why-us-woman-are-deleting-their-period-tracking-apps
Germain, Thomas. 2021. "Mental Health Apps Aren't All as Private as You May Think." *Consumer Reports*, March 2. https://www.consumerreports.org/health/health-privacy/mental-health-apps-and-user-privacy-a7415198244/
Germain, Thomas. 2022. "Guess What? HIPAA Isn't a Medical Privacy Law." *Consumer Reports*, June 13. https://www.consumerreports.org/health/health-privacy/guess-what-hipaa-isnt-a-medical-privacy-law-a2469399940/
Goodwin, Michelle. 2020. *Policing the Womb: Invisible Womena Nd the Criminalization of Motherhood*. New York: Cambridge University Press.
Halva-Neubauer, Glen. A., and Sara L. Zeigler. 2010. "Promoting Fetal Personhood: The Rhetorical and Legislative Strategies of the Pro-Life Movement After *Planned Parenthood V. Casey*." *Feminist Formations* 22 (2):101–23. doi:10.1353/ff.2010.0011.
Hamilton, Isobel Asher, and Dominick Reuter. 2022. "You Shouldn't Feel You Have to Delete Your Period-Tracking App Because Roe V. Wade Was Overturned — but You Should Know the Risks, Expert Says." *Business Insider*, June 24. https://www.businessinsider.com/should-i-delete-period-tracking-app-roe-wade-overturned-privacy-2022-5
Hill, Kashmir. 2023. "Deleting Your Period Tracker Won't Protect You." *New York Times*, June 22. https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html
Howard, Grace. 2020. "The Pregnancy Police: Surveillance, Regulation, and Control." *Harvard Law & Policy Review* 14 (2): 347–64.
Kalish, Lil. 2022. "Meet Abortion Bans' New Best Friend—Your Phone." *Mother Jones*, February 16. https://www.motherjones.com/politics/2022/02/meet-abortion-bans-new-best-friend-your-phone/
Kang, Jerry. 1998. "Information Privacy in Cyberspace Transactions." *Stanford Law Review* 50 (4):1193–294. doi:10.2307/1229286.
Kavi, Aishvarya. 2021. "How the HIPAA Law Works and Why People Get It Wrong." *New York Times*, July 24. https://www.nytimes.com/article/hipaa-law.html
KFF. 2019. "Health Apps and Information Survey." *Henry J. Kaiser Family Foundation*, September 10. https://www.kff.org/other/poll-finding/kff-health-apps-and-information-survey/
Koepke, Logan, Emma Weil, Urmila Janardan, Tinuola Dada, and Harlan Yu. 2020. "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones." *Upturn*, October 20. https://www.upturn.org/work/mass-extraction/
Levy, Karen E C. 2015. "Intimate Surveillance." *Idaho Law Review* 51 (3): 679–94.
Moglia, Michelle L., Henry V. Nguyen, Kathy Chyjek, Katherine T. Chen, and Paula M. Castaño. 2016. "Evaluation of Smartphone Menstrual Cycle Tracking Applications Using an Adapted APPLICATIONS Scoring System." *Obstetrics & Gynecology* 127 (6):1153–60. doi:10.1097/AOG.0000000000001444.
Morrison, Sara. 2022. "Should I Delete My Period App? And Other Post-Roe Privacy Questions." *Vox*, July 6. https://www.vox.com/recode/2022/7/6/23196809/period-apps-roe-dobbs-data-privacy-abortion
Myers, Caitlin Knowles. 2022. "Confidential and Legal Access to Abortion and Contraception in the USA, 1960–2020." *Journal of Population Economics* 35 (4):1385–441. doi:10.1007/s00148-022-00902-4.
Nash, Elizabeth, and Megan K Donovan. 2019. "Ensuring Access to Abortion at the State Level: Selected Examples and Lessons." *Policy Review* 22: 1–7.
Nash, Elizabeth, and Isabel Guarnieri. 2023. "Six Months Post-Roe, 24 US States Have Banned Abortion or are Likely to Do So: A Roundup." *Guttmacher Institute* January. https://www.guttmacher.org/2023/01/six-months-post-roe-24-us-states-have-banned-abortion-or-are-likely-do-so-roundup.
New York Times. 2023. "Tracking Abortion Bans Across the Country." *New York Times*, December 8. https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html
Ohm, Paul. 2010. "Broken Promises of Privacy." *UCLA Law Review* 57: 1701.

Pew Research Center. 2022. "America's Abortion Quandry." *Pew Research Center*, May 6. https://www.pewresearch.org/religion/2022/05/06/americas-abortion-quandary/

Roberti, Amanda. 2022. "Empowering Women by Regulating Abortion? Conservative Women Lawmaker's Cooptation of Feminist Language in US Abortion Politics." *Politics, Groups & Identities* 10 (1):139–45. doi:10.1080/21565503.2021.2003828.

Roberts, Catherine. 2022. "These Period Tracker Apps Say They Put Privacy First. Here's What We Found." *Consumer Reports*, May 25. https://www.consumerreports.org/health/health-privacy/period-tracker-apps-privacy-a2278134145/

Rosenberg, Gerald N. 1991. *The Hollow Hope: Can Courts Bring About Social Change?* Chicago: Chicago University Press.

Schwartz, Paul M. 1999. "Privacy and Democracy in Cyberspace." *Vanderbilt Law Review* 52:1607. doi:10.2139/ssrn.205449.

Shipp, Laura, and Jorge Blasco. 2020. "How Private is Your Period? A Systematic Analysis of Menstrual App Privacy Policies." *Proceedings on Privacy Enhancing Technologies* 2020 (4): 491–510.

Siegel, Reva. 1992. "Reasoning from the Body: A Historical Perspective on Abortion Regulation and Questions of Equal Protection." *Stanford Law Review* 44 (2):261–381. doi:10.2307/1228947.

Tiffany, Kaitlyn. 2018. "Period-Tracking Apps are Not for Women." *Vox*, November 16. https://www.vox.com/the-goods/2018/11/13/18079458/menstrual-tracking-surveillance-glow-clue-apple-health

Torchinsky, Rina. 2022. "How Period Tracking Apps and Data Privacy Fit into a Post-Roe V. Wade Climate." *NPR*, June 24. https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps

Tschinkel, Arielle. 2022. "Should I Delete My Period Tracking App? Why Reproductive Surveillance is a Big Concern." *Scary Mommy* [blog], July 28. https://www.scarymommy.com/lifestyle/are-period-tracking-apps-safe

Turow, Joseph Yphtach Lelkes, Nora A. Draper, and Ari Ezra Waldman. 2023. "Americans Can't Consent to Company's Use of Their Data." *Annenberg School for Communication - University of Pennsylvania*. https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf.

Vestal, Christine. 2023. "First State Law to Criminalize Abortion 'Trafficking' May Inspire Others." *Stateline*, April 7. https://stateline.org/2023/04/07/first-state-law-to-criminalize-abortion-trafficking-may-inspire-others/

Worsfold, Lauren, Lorrae Marriott, Sarah Johnson, and Joyce C Harper. 2021. "Period Tracker Applications: What Menstrual Cycle Information are They Giving Women?" *Women's Health* 17 (January):174550652110499. doi:10.1177/17455065211049905.

Ziegler, Mary. 2014. "Beyond Backlash: Legal History, Polarization, and Roe V. Wade." *Washington and Lee Law Review* 71 (2): 969–1024.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Appendix

Table A1. Application Statistics.

Policy Name	Application Name	Google or Apple	Lifetime US Downloads	Lifetime Global Downloads
28Wellness	28 Period Tracker & Fitness	Both	200K+	500K+
Clover	Period & Cycle Tracker – Clover	Both	200K+	5 M+
Clue	Clue Period Tracker & Calendar	Apple	12 M+	40 M+
			10 M+	20 M+
		Google	2 M+	5 M+
Femia	Ovulation & Fertility – Femia	Both	200K+	500K+
Femometer	Femometer Fertility Tracker	Apple	2.2 M+	10 M+
	Bongmi Global Group		2 M+	5 M+
	Femometer Limited	Both	200K+	5 M+
Flo	Flo Period and Pregnancy Tracker	Both	20 M+	100 M+
Glow			10 M+	15 M+
	Glow: Fertility, Ovulation App	Both	5 M+	5 M+
	Period Tracker – Eve	Both	5 M+	10 M+
GP Apps	Period Tracker by GP Apps	Both	10 M+	20 M+
	Period Tracker HD	Apple		
	Period Tracker Deluxe	Both		
Heena	Heena Health	Google	<5K	200K+
Leap[1]			10 M+	100 M+
	Period Calendar Period Tracker	Google		
	Period Tracker Period Calendar	Apple		
	Ovulation & Period Tracker Period Calendar Pro	Google		
		Google		
MeetYou[2]	MeetYou – Period Tracker	Both	500K+	50 M+
Menstrual Cycle			1 M+	5 M+
Tracker	Menstrual Cycle Tracker	Both		
	Fertility & Period Tracker	Apple		
	Fertility and Period Tracker Menstrual Periods Tracker	Apple Apple		
	Fertility Tracker for Women	Apple		
My Calendar			2 M+	20 M+
	My Calendar – Period Tracker	Both		
	Period Tracker & Diary	Google		
	Cycle Tracker: Period Calendar	Apple		
NaturalCycles	Natural Cycles App	Apple	1 M+	2 M+
Ovulation	Ovulation Calendar and Fertility	Google	200K+	2 M+
Calendar				
PepApp	PepApp	Both	20K+	5 M+
Period Tracker	Period Tracker – Cycle Tracker	Apple	5K+	50K+
PinkBird	Period tracker by PinkBird	Google	100K+	5 M+
PregTest&Tracker	Pregnancy Test & Tracker	Google	20K+	1 M+
Spot On	Spot On Period Tracker	Both	2 M+	2 M+
Stardust	Stardust Period Tracker	Both	1 M+	1 M+
WoCute	WoCute – Period Calendar	Both	100K+	5 M+
WomanLog			500K+	5 M+
	WomanLog Calendar	Both		
	WomanLog Pro Calendar	Both		

[1]Totals include these four apps, plus a Chinese version available for both Apple and Google.
[2]Summary of three apps, English version available for both Apple and Google, and Chinese version available for Apple.