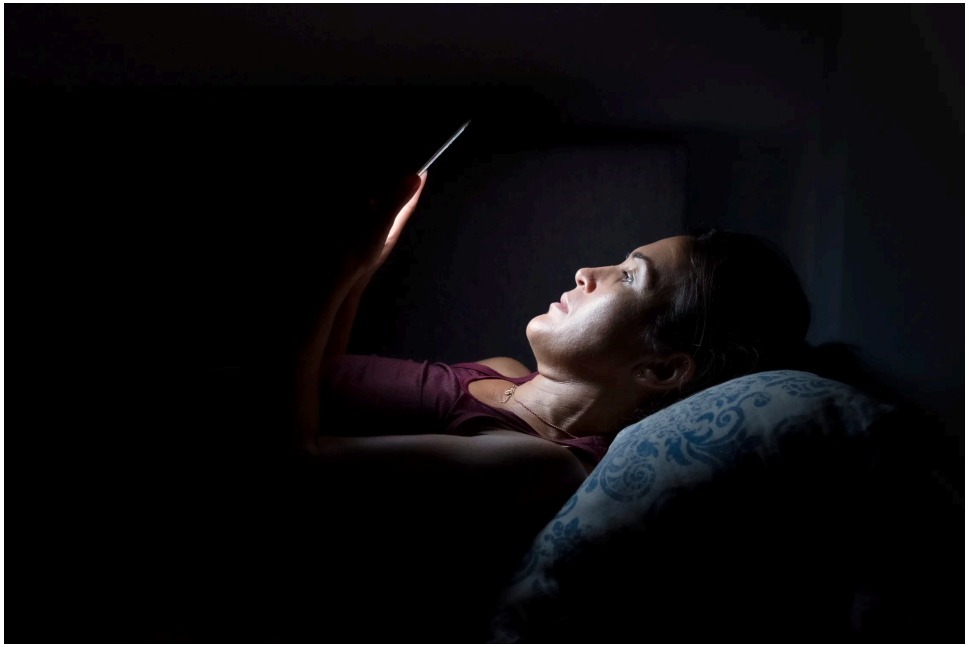
KRISTEN POLI SECURITY JUL 28, 2022 7:00 AM

The Most Popular Period-Tracking Apps, Ranked by Data Privacy

Under increased scrutiny, certain period-tracking apps are seeing a surge of new users. Which are as safe as they claim to be?



PHOTOGRAPH: IMAGINESTOCK/GETTY IMAGES

IN THE WAKE of the Supreme Court's decision to overturn *Roe v. Wade*, tens of thousands of Americans have turned to their smartphones to share information and assess their app libraries. Legal experts have warned that people seeking abortion care have become critically vulnerable to privacy threats, especially those who reside in states where "bounty hunter" laws incentivize private citizens to file civil complaints against them.

As a response, many people have sought out more dependable and secure ways to track their menstrual cycles via period-tracking apps, despite a recent flurry of tweets urging users to delete them en masse. Period-trackers, a subcategory of mobile health (mHealth) apps, have grown extremely popular over the years, with one 2019 Kaiser Family Foundation study counting a third of American women as users.

App store data suggests that this number has grown even higher since the Supreme Court's decision was released. Reports from Data.ai, which tracks install and use data for app developers and other companies, show that the top five period-tracking apps in the US improved their app store rankings by an average of 48 percent between June 24th and June 30th of this year, suggesting a large spike in downloads. Two particular apps, Stardust and Clue, raced to the top of the charts with breakneck speed, doubling their prominence across Google Play and Apple's App

Store rankings in a single week. This points to the idea that users aren't abandoning their period-tracking apps so much as trading them in for new ones.

This is due in part to new press releases from mHealth category leaders, who promised readers that enhanced safety and data privacy measures for their own apps were either completed or well underway. Relative newcomer Stardust—which was just released last Thursday—said in a recent announcement: "We do not sell data. We have never sold data. We will never sell data." The company's privacy policy, however, indicates they may freely hand over data to authorities on request, without a warrant or notifying the user. Leadership at Clue, a popular period-tracker based in Germany, also stressed their commitment to refrain from "responding to any disclosure request or attempted subpoena of our users' health data by US authorities."

How seriously should users take these statements, especially when they may conflict with the service's own policies? What really makes a period-tracker app safe to use? To find out, we analyzed the privacy policies of the 5 most popular period-tracking apps in the US: Flo, Clue, Stardust, Period Calendar, and Period Tracker (these earned the highest number of downloads in 2022, according to AppMagic).

While claims made within privacy policies are enforceable under the Federal Trade Commission Act, health-related information collected by apps is not inherently protected "by any meaningful privacy law," according to Alexandra Reeve Givens, president & CEO of the Center for Democracy & Technology (CDT), a 501 nonprofit based in Washington, DC. This includes HIPAA. "HIPAA only protects information that's being collected and owned by a medical provider, or similar covered entity," Givens notes.

This not only shifts the burden of risk assessment to individual users, but also makes evaluating the privacy and security of apps difficult to begin with. To do so, we consulted evaluation frameworks pioneered by the Beth Israel Deaconess Medical Center (MIND) and The Digital Standard to arrive at four core questions to guide our study.

	Does the app store data locally?	Does the app share information with third-parties?	Does the app allow you to delete your data?	Does the app track your location?	SCORE
FLO	No (0)*	Yes, clearly specifies what information is shared.** (1)	Yes, but retention period is unspecified. (2)	Yes. May send IP address to 3rd parties. (1)	**4**
CLUE	No (0)	Yes, clearly specifies what information is shared.* (1)	Yes, but 30 day retention period applies. Extends to third parties. (3)	Yes. May send IP address to 3rd parties. (1)	**5**
STARDUST	No (0)	No, does not clearly specify what information is shared.* (0)	Yes, but retention period is unspecified. (2)	Yes. May send IP address to 3rd parties. (1)	**3**
PERIOD CALENDAR PERIOD TRACKER	No (0)	No, does not clearly specify what information is shared.* (0)	Yes, but retention period is unspecified. (2)	Yes, uses location tracking. (0)	**2**
PERIOD TRACKER BY PG APPS	No (0)	No, does not clearly specify what information is shared.* (0)	Yes, but with 2-year retention period applies. Continued storage in aggregate. (1)	Yes, uses location tracking. (0)	**1**

*A score of (0) = the app did not fulfill the privacy requirement, (1) = the app partially fulfilled the privacy requirement, (2) = the app fulfilled the privacy requirement, and (3) = the app fulfilled the privacy requirement well
**'Clear specification' is defined here as an index of third-party companies and the data they receive

*A score of (0) = the app did not fulfill the privacy requirement, (1) = the app partially fulfilled the privacy requirement, (2) = the app fulfilled the privacy requirement, and (3) = the app fulfilled the privacy requirement well **'Clear specification' is defined here as an index of third-party companies and the data they receive.

Local vs. Cloud Storage

Understanding *where* companies store your data is pivotal to assessing the privacy risk that comes with using their products. Most popular mobile apps store user data in the cloud—across multiple servers in multiple locations—which allows them to process large amounts of easily recoverable information. It also means that your data is more vulnerable to bad actors. This is why organizations like Givens' prefer apps that store information directly on users' devices. If an app stores data directly on your mobile phone, you'll have more complete control of it. None of the apps reviewed above gave users the option to store their data locally, but Euki and Mozilla Foundation-backed Drip do.

Third-Party Sharing

If you've used Facebook to log in to a website or app recently, you're already familiar with some of the ways that app developers share information with third parties. Understanding which third parties a company works with and what type of data is passed on to them is a helpful way to evaluate your level of protection. For example, Period Tracker's privacy policy admits to sharing users' device IDs with advertising networks, which is quite risky. It also expresses their willingness to sell or transfer user data as a result of a corporate merger or sale. Typically, apps who lay out plainly who they're providing info to and why—like Clue does —are more trustworthy.

It's also helpful to know whether data is routinely anonymized (stripped of identifying user information) before being shared with these third parties. However, this isn't a panacea. Stripped-down data can still lead back to individual users under certain conditions. Machine learning makes this threat even more real, since the technology can speed up shady "re-identification" processes. Despite vowing to refrain from sharing user data themselves, Clue passes on anonymized data to certain third-party research groups. While Stardust expresses a commitment to limiting the information they share with third parties, their policy states it could share information in order to "comply with or respond to law enforcement," or to protect the "security of the Company." Ideally, apps are extremely selective with which third-parties they're willing to share info with—or they don't share with third-parties at all.

Data Deletion

Every app should have established protocols that allow users to delete their personal data from the developers' systems at will. While many US-based apps include these protocols to comply with the EU's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), users should look out for privacy policies that *clearly* extend these erasure privileges to all users, regardless of location. Even so this can be tricky, says Givens: "If you're not a resident of the jurisdiction that the law is covering, there's no guarantee that they are going to honor it."

Even apps that invite data deletion requests may not always execute them in a timely or complete fashion. Flo, whose security practices placed them under FTC scrutiny in 2021, states specifically in their privacy policy that upon deletion of their app, they "retain your personal data for a period of 3 years in case you decide to re-activate." Period Tracker admits to retaining users' mobile device IDs "for up to 24 months" after receiving a request. The safest apps should retain your data for 30 days or less, and ideally submit deletion requests to third parties on your behalf, like Clue does.

Location Tracking

If an app explicitly stores location data (like Period Calendar and Period Tracker do) it presents a greater privacy issue. While three out of the five apps analyzed here didn't appear to save location data explicitly, each app saves users' IP addresses, which can be used to determine someone's general location. Flo, for example, explicitly shares IP addresses with third-parties such as AppsFlyer.

Stardust's practices decouple users' IP addresses from their health data, which increases security. But critics say their methods fall short of true end-to-end encryption. Regardless, when IP addresses are combined with outside data, such as a user's search history or even other publicly available information about the user, they can easily reveal that person's identity and their activities. The CDT and other privacy advocates have warned that users' text messages and search histories have already been used against them in legal proceedings involving their reproductive health, and the practice is likely to expand.

The Bottom Line

At the end of the day, a period-tracking app like Clue presents users with slightly less risk than apps like Flo, Stardust, Period Calendar, and Period Tracker. However, all five of these apps, chosen for their outsize popularity, falter when compared with more secure options like Euki and Drip, as corroborated by Consumer Reports. Insofar as it's possible for users to analyze *all* of their apps according to standards set forth in The Digital Standard, Mhealth Index, and elsewhere, users can make educated decisions about which companies to align with—but evaluating the risks of using specific apps is an imperfect science. In addition to being extremely time consuming and often confusing, it's nowhere near a suitable replacement for a lack of widespread legal privacy protections available for all Americans.

WOMEN'S HEALTH

Period-Tracking and Fertility Apps Can Put Women Seeking Abortions at Risk

VITTORIA ELLIOTT

KNOW YOUR RIGHTS

A Guide to Abortion Resources in a Post-*Roe* America

LUX ALPTRAUM

REPRODUCTIVE RIGHTS

The Story of Abortion Pills and How They Work

CHRIS BARANIUK

According to privacy experts like Givens, period-tracking apps represent the tip of the iceberg when it comes to digital privacy and security post-*Roe*. The CDT recommends that people assess their own risk level in order to determine whether using a period-tracking app is even worth it. In the meantime, taking steps to secure your personal information like text messages and search histories is probably more worthwhile.

For those looking to make a difference, experts recommend advocating directly to tech companies, especially precedent-setting organizations like Google and Meta

(formerly Facebook) to demand better individual protections. It's these corporations that will eventually have to respond to requests from law enforcement for user data, and many already promise to curtail their surveillance (but also lobby aggressively against privacy legislation and regulation). To pave the way for better policy, tech companies should aim to take serious inventory of the data they're collecting, file transparency reports regularly, and, most importantly, take public stances in defense of privacy rights early and often.

You Might Also Like ...

- **In your inbox:** Get Plaintext—Steven Levy's long view on tech
- Musk takeover: No, 150-year-olds aren't collecting benefits
- **Big Story:** Are you lonely? Adopt a new family on Facebook today
- The wild story behind Kendrick Lamar's Super Bowl halftime show
- **Love Bytes:** The brave new frontiers of romance

Kristen Poli is a freelance writer interested in travel and technology. She is a PhD candidate at Trinity College and lives in Dublin. ... Read more

CONTRIBUTOR

TOPICS PRIVACY APPS REPRODUCTIVE RIGHTS ENCRYPTION DATA PRIVACY