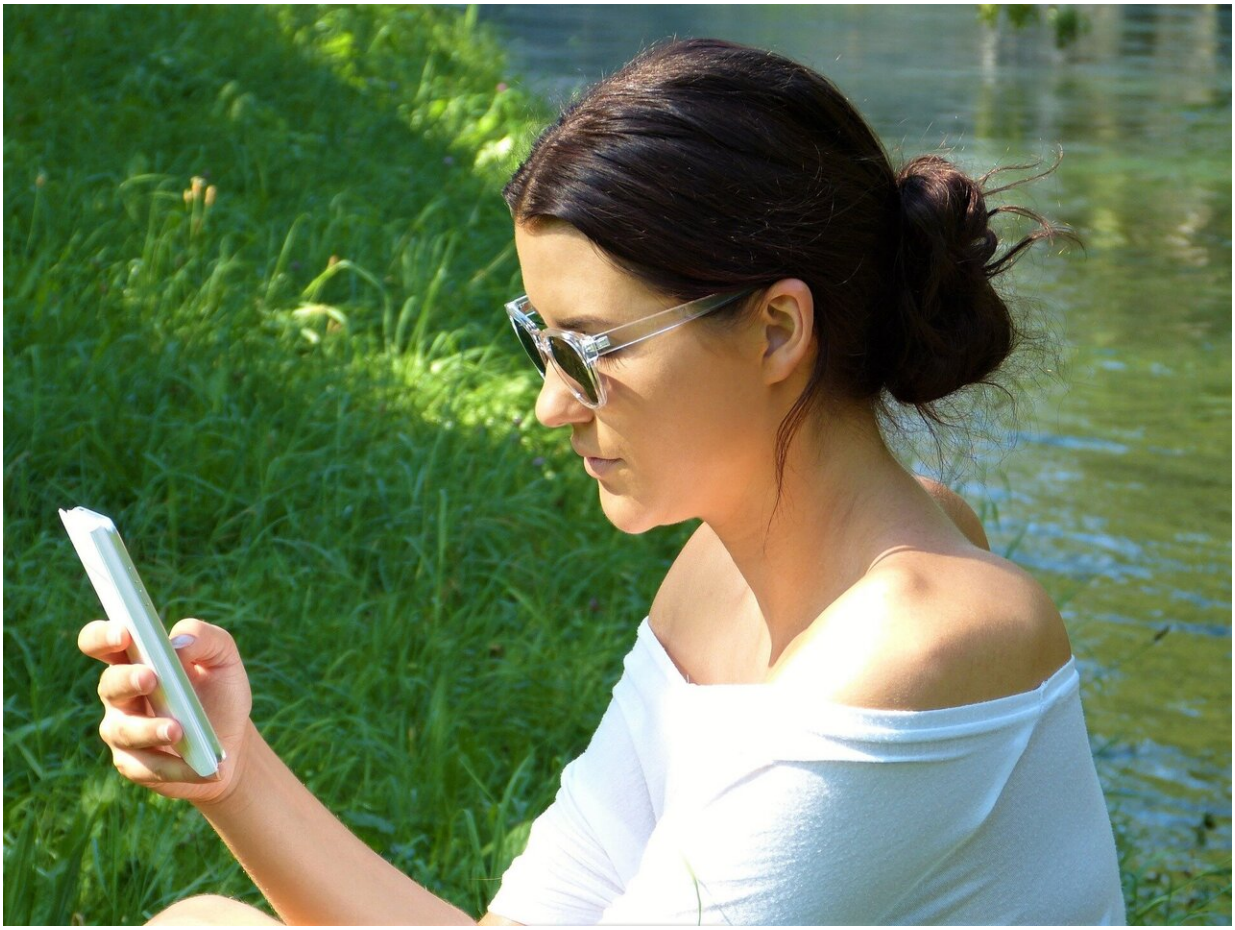
Should you worry about data from your period-tracking app being used against you?

May 16 2022, by Hannah Norman and Victoria Knight



Credit: Pixabay/CC0 Public Domain

It's estimated that millions of people in the U.S. use period-tracking apps

to plan ahead, track when they are ovulating, and monitor other health effects. The apps can help signal when a period is late.

After Politico published on May 2 a draft opinion from the Supreme Court indicating that Roe v. Wade, the law that guarantees the constitutional right to an abortion, would be overturned, people turned to social media. They were expressing concerns about the privacy of this information—especially for people who live in states with strict limits on abortion—and how it might be used against them.

Many users recommended immediately deleting all personal data from period-tracking apps.

"If you are using an online period tracker or tracking your cycles through your phone, get off it and delete your data," activist and attorney Elizabeth McLaughlin said in a viral tweet. "Now."

Similarly, Eva Galperin, a cybersecurity expert, said the data could "be used to prosecute you if you ever choose to have an abortion."

That got us wondering—are these concerns warranted, and should people who use period-tracking apps delete the data or the app completely from their phones? We asked the experts.

Is your period-tracking app data shared?

Privacy policies—specifically, whether the apps sell information to data brokers, use the data for advertising, share it for research, or keep it solely within the app—vary substantially among companies.

"Does it encrypt? What's its business model?" said Lucia Savage, chief privacy and regulatory officer for Omada Health, a digital therapeutics company. "If you can't find terms of service or a privacy policy, don't

use that app."

Period-tracking apps are often not covered under the Health Insurance Portability and Accountability Act, or HIPAA, though if the company is billing for health care services, it can be. Still, HIPAA doesn't prevent the company from sharing de-identified data. If the app is free—and the company is monetizing the data—then "you are the product" and HIPAA does not apply, Savage said.

A 2019 study published in the *BMJ* found that 79% of health apps available through the Google Play store regularly shared user data and were "far from transparent."

When it comes to marketing, a pregnant person's data is particularly of high value and can be hard to hide from the barrage of cookies and bots. Some period-tracking apps, which often ask for health information besides menstrual cycle details, take part in the broader internet data economy, too.

"The data can be sold to third parties, such as big tech companies; or to insurance companies, where it could then be used to make targeting decisions, such as whether to sell you a life insurance policy, or how much your premium should be," said Giulia De Togni, a health and artificial intelligence researcher at the University of Edinburgh in Scotland.

Flo Health, headquartered in London, settled with the Federal Trade Commission last year over allegations that the company, after promises of privacy, shared health data of users using its fertility-tracking app with outside data analytics companies, including Facebook and Google.

In 2019, Ovia Health drew criticism for sharing data—though de-identified and aggregated—with employers, who could purchase the

period- and pregnancy-tracking app as a health benefit for their workers. People using the employer-sponsored version must currently opt in for this kind of data-sharing.

Ovia's roughly 10,000-word privacy policy details how the company may share or sell de-identified health data and uses tracking technologies for advertisements and analytics on its free, direct-to-consumer version.

For European residents, companies must comply with the stricter General Data Protection Regulation, which gives ownership of data to the consumer and requires consent before gathering and processing personal data. Consumers also have the right to have their online data erased.

Companies have the option of extending those rights to people living in the U.S. via their privacy policies and terms of services. If they do so, the FTC can then hold the companies accountable for those commitments, said Deven McGraw, Invitae's head of data stewardship and the former deputy director for health information privacy at the Department of Health and Human Services Office for Civil Rights.

The period-tracking app Cycles, which is owned by Swedish company Perigee, falls into this category. The company promises its users that it does not do any advertising or selling of data to third parties. Instead, it makes money solely through subscriptions, spokesperson Raneal Engineer said.

Concerned customers have been reaching out to another health app, Clue, developed by a company based in Berlin. "We completely understand this anxiety, and we want to reassure you that your health data, particularly any data you track in Clue about pregnancies, pregnancy loss or abortion, is kept private and safe," Clue co-CEO Carrie Walter said in an emailed statement.

Some states, such as California and Virginia, have state-level laws that give users ownership over their information and whether it is sold to third parties.

Data brokers trade in other types of information, such as location-tracking data for people who visited Planned Parenthood, which potentially could be purchased by law enforcement or government officials. Earlier this month, SafeGraph halted selling cellphone-tracking data mapping the movements of people visiting Planned Parenthood, how long they stayed, and where they went afterward, after Vice reported buying a week's worth of data for $160.

Also of concern is a company's level of data security, and how susceptible it is to a breach. "Hacking is criminal, there's no question about it," Savage said. "But once it's hacked, information can be released."

Could this data be used in a criminal prosecution?

The short answer is yes.

"It's almost surreal that in some states using a period app could get you into trouble," said McGraw. "But if an abortion is a crime, it could be accessed in building a case against you."

This depends on where you live, but there are no federal protections against that happening from a privacy standpoint, she added. Last year, Sen. Ron Wyden (D-Ore.) introduced the Fourth Amendment Is Not For Sale Act, which would prohibit data brokers from selling personal information to law enforcement or intelligence agencies without court oversight. But the legislation has yet to make it to a vote.

Wyden told KHN he was "absolutely" worried about the chance that

people who seek an abortion could be incriminated by their phone data.

"It is really an ominous prospect of women having their personal data weaponized against them," said Wyden. "These big data outfits," he said, "gotta decide—are they going to protect the privacy of women who do business with them? Or are they basically going to sell out to the highest bidder?"

In the absence of a federal law, if law enforcement does get a court-ordered subpoena, it can be difficult for a company to resist handing over data related to a specific case.

"Given the breadth of surveillance laws in the U.S., if a company collects and keeps information, that information is susceptible to being compelled by law enforcement," said Amie Stepanovich, a privacy lawyer and vice president of U.S. policy at the Future of Privacy Forum. "They don't necessarily have the ability to legally keep that information from law enforcement once the proper process has been undertaken."

Still, even in states with strict abortion limits on the books, much depends on how those laws are structured. Last month, for instance, a murder charge against a Texas woman for a "self-induced abortion" was dismissed after the district attorney found it did not violate state law, which criminalizes providers performing abortions, not the patients.

If Roe v. Wade is struck down, 14 states have so-called trigger laws that would automatically go into effect and ban abortion outright or after set windows of time—for instance, six weeks or 15 weeks, according to a KFF analysis.

"It's really complicated under the hood, but I don't think people should blindly assume their data is safe from legal process," Savage said. It can depend on the company's approach to subpoenas, she added. Some will

fight them while others will not.

Take Apple, for example, which repeatedly resisted unlocking iPhones for law enforcement in high-profile cases like the 2015 San Bernardino shooting. Data in Apple's health app, which includes its period tracker, is "encrypted and inaccessible by default," according to the company's privacy policy. All the health data in the app is kept on a person's phone, not stored on servers. But at the same time, Savage said, people who are in low-income communities don't always have an iPhone because it is an expensive piece of equipment.

Ovia's privacy policy says the company may give data to law enforcement if required by law or subpoena. The company, however, said in a statement that it has "never provided Ovia user data to any government, nor have we ever received any government requests for access to Ovia user data." There is also an option in Ovia's account settings to delete account data "entirely and permanently."

Despite safeguards in place under the GDRP, period trackers based in Europe can still be subpoenaed as well, said Lee Tien, a senior staff attorney at the Electronic Frontier Foundation.

"Even [European Union] companies are subject to the U.S. legal process, though it would take longer," said Tien. "The U.S. has mutual legal treaties with other countries, including E.U. countries, and law enforcement knows how to exchange information."

Has this kind of information been used by public officials or law enforcement before?

Officials holding anti-abortion views have leveraged period-tracking information in the past. In 2019, former Missouri state health director

Dr. Randall Williams obtained a spreadsheet tracking the menstrual periods of women who visited Planned Parenthood in an effort to identify patients who had experienced an abortion that failed to terminate the pregnancy.

During the Trump administration, former refugee resettlement chief and anti-abortion activist Scott Lloyd admitted to keeping track of the menstrual cycles of teen migrants in an effort to stop them from getting abortions.

"We are now thinking of period trackers the way we've been thinking of facial recognition software for years," Savage said.

Should you delete your period-tracking app?

Experts said it's unlikely that a period-tracking app would be the sole piece of evidence used if someone were building a case against you for seeking an abortion.

"Frankly, I think if law enforcement or a civil investigator were trying to figure out who is having an abortion, there are probably several other venues that are more realistic or more immediately useful," said Stepanovich. "They would likely get a dump of information for the relevant data," she continued, "such as trying to get the location information of everyone that got dropped off close to an abortion center, which is a much smaller set of data, or getting people who called abortion hotlines at certain times."

Stepanovich added that as long as someone is using a smartphone with any type of app on it there is a risk that data could be obtained and used as part of a criminal or civil prosecution. Bottom line: The only way to avoid risk altogether is to not use a smartphone.

But McGraw took a more cautious approach: "If I lived in a state where I thought that data might end up in the hands of law enforcement, I wouldn't track [my period] at all."

Ultimately, people who use period-tracking apps should be aware of the risk of using the technology while considering the benefit it brings to their life.

"You have to think about what you need in terms of period tracking," said Tien. "You have to weigh and ask yourself, 'How much does this convenience really matter to me?'"

2022 Kaiser Health News.
Distributed by Tribune Content Agency, LLC.

Citation: Should you worry about data from your period-tracking app being used against you? (2022, May 16) retrieved 17 July 2024 from https://medicalxpress.com/news/2022-05-period-tracking-app.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.