From Menstruation to Regulation: Understanding Data Privacy Laws and Period Tracker Apps

Kate Braddom

https://doi.org/10.4079/pp.v31i0.14

This previously appeared on Brief Policy Perspectives in February 2024 and was not subject to the same review process as our peer-reviewed journal articles.

In the era of online dating, wearable technologies and virtual workspaces, the emergence of 'digital contraceptives' seems almost inevitable. Especially as online sources of medical information and telehealth have begun to fill gaps in access to care, these technologies have become particularly important for many people. But these technologies also pose serious risks in a post-Roe v. Wade era — they collect extremely detailed data about women's bodies, reproductive health and menstrual cycles, and the ways in which this data is used, both by private companies and law enforcement, is legally murky. There has been a lot of concern from users about the potential for the digital data of pregnant people to be used to prosecute them in anti-abortion cases (Dong et al. 2022). What data privacy protections do pregnant people have in the United States? Is it really possible that that data could be used to criminalize them?

DATA PRIVACY IN THE UNITED STATES

The United States currently has few data privacy protections in place for individuals. At the federal level, data privacy laws are a relatively weak and patchwork set of policies that mainly target specific types of data or specific populations. For instance, the Fair Credit Reporting Act outlines protections for credit report data (Federal Trade Commission 2013a), the Family Educational Rights and Privacy Act (FERPA) regulates access to student education records (U.S. Department of Education 2021), and the Children's Online Privacy Protection Rule (COPPA) limits what companies can do with data collected from or about children under 13 years of age (Federal Trade Commission 2013b). However, there is no comprehensive federal legislation that governs data more generally, meaning that for the most part, companies can collect, store or share your data in any way they want with whomever they want, and data usage is not limited to targeted advertising (Klosowski 2021). Some companies have reportedly used personal data to inform insurance policies or even adjust interest rates based on an individual's race. In addition, companies often do not have to notify you when they share or sell your data, and third parties that obtain your data

can continue to sell or share it without your knowledge or consent, which means that people generally have no idea who actually has access to their data.

Some states have or are developing more comprehensive data privacy laws, but these laws vary widely. Three states have already enacted comprehensive legislation, most notably California and Virginia. California's Consumer Privacy Act of 2018 (California Privacy Protection Agency 2018) is widely considered to be the strictest data privacy law in the country and is modeled off of the European Union's General Data Protection Regulation (GDPR) (Wolford 2018), which has now become a kind of international gold standard for data privacy regulation (Dresner 2024). California's law includes a limited "private right of action" which enables individuals to sue companies for certain types of data breaches, as well as a "global opt-out" provision in which individuals have the ability to remove themselves from data sharing by device or browser, rather than having to opt-out of each website separately (New America 2024). In addition, California's law gives consumers the right to know what personal information is being collected about them, whether that information is being sold and to whom, and the right to delete information that is collected from them. Virginia's Consumer Data Protection Act on the other hand, is relatively weak (Virginia Legislative Information System 2024). It does not include a private right to action and provisions generally allow data-gatherers to continue collecting from consumers without significant changes.

DATA PRIVACY FOR PERIOD TRACKERS

Apps that monitor and predict periods may not be as secure as some users expect. To start, despite the fact that these apps explicitly collect and store health information, they are not protected by HIPAA. HIPAA is designed to apply only to "covered entities," like hospitals and health insurance plans. Since these apps are not included in the law as covered entities, they do not have to adhere to HIPAA's standards when handling health data. An in-depth analysis of data privacy for 35 period tracking apps, published in 2023, conducted traffic analyses and reviewed apps' privacy policies and practices, finding that many apps are collecting sensitive information about their users (Dong et al. 2022). In addition to just updating a menstrual calendar, many apps encourage women to enter data like body temperature, weight, moods, PMS symptoms, and pregnancy information to inform features like due date calculators. In addition to collecting sensitive information, 16 apps include explicit statements in their privacy policies stating that they may disclose users' personal data to law enforcement or government agencies in response to subpoenas or court orders. Even anonymized data is often not entirely secure. Some apps collect location data, unbeknown to the user, which can be used to de-anonymize data and tie it to a specific user. Even when period tracking apps do not collect location data, many of them require users to create an account with identifying details including their name, date of birth and contact information. In addition to sharing data with law enforcement, the companies behind tracking apps often sell the data to third parties. In 2021, a complaint from the Federal Trade Commission alleged that Flo Health shared health data of millions of users with third party marketing

and analytics firms including both Facebook and Google's analytics divisions, despite Flo's privacy policy assuring users that their health data would be kept private (Jillson and Plant 2021). Flo also did not limit how third parties could use the health data being shared, which means the data could continue to be bought and sold for other purposes.

DIGITAL DATA IN ABORTION PROSECUTIONS

Can digital data from these apps really be used in abortion prosecutions? While there have not been any cases yet, law enforcement has used other forms of digital data in similar cases. In the case of Latice Fisher, who was prosecuted for the death of her 35-week-old fetus, her digital data gave prosecutors a "window into [her] soul" that helped to establish intent and support the prosecutor's general theory that Fisher did not want the fetus to survive (Conti-Cook 2020). While data from period tracker apps does not necessarily prove that someone had an abortion, the existence of extremely detailed data about a person's menstrual cycles and reproductive health can be used to legally establish intent, as in the Fisher case, or to surveille certain individuals or groups in order to identify suspects. For instance, prosecutors no longer have to rely on reports from medical staff to identify individuals suspected of terminating a pregnancy. Instead, prosecutors could potentially subpoena internet service providers for the IP addresses of anyone who searched a specific keyword combination, such as "how to have an abortion," or the state can simply purchase data from a third party. This means that prosecutors could obtain large sets of data from a period tracker app to identify anyone who's menstrual data indicates that they were pregnant.

In many cases, a court order is also not necessary for government agencies to obtain sensitive data. There are some cases of federal agencies purchasing data for surveillance purposes. Federal immigration officials have been able to purchase data related to immigrants' menstrual cycles without a warrant in order to monitor for pregnancies (Conti-Cook 2020). Additional data like online search histories, website navigation histories and purchasing histories could also be obtained in the same way and used to identify suspects.

FUTURE OF PRIVACY PROTECTIONS

Some apps are taking steps to protect users' information. Flo recently announced the launch of a new 'anonymous mode' that will allow individuals to use the app without any personally identifying information associated with their account, which would make it much more difficult to de-anonymize health data.

Federal data privacy legislation has been proposed, but it is still in the early stages and many provisions face strong opposition from lobbyists representing tech companies (Klosowski 2021). A number of bills at the state level have already failed to pass because authors included a private right of action, and the Internet Association, which represents big tech companies like Amazon, Facebook, and Google, is actively pushing to maintain the current opt-out consent model and to require individuals to opt-out of data sharing manually for

every website.

There have also been some limited efforts to protect sensitive data from law enforcement. In 2021, Sen. Ron Wyden (D-Ore.) introduced the Fourth Amendment is Not For Sale Act, which would prohibit companies from selling user data to law enforcement agencies without court oversight (Wyden 2021). The bill would also prevent data that is collected or shared in a way that violates a platform's service agreement or privacy policy from being used as evidence. Unfortunately, the bill has never been voted on, and would be unlikely to pass. Despite privacy concerns, digital contraceptives do provide new ways for women to manage their reproductive health free of the risks and side effects of other forms of birth control, and they enable women to gain a new understanding of their bodies that allow them to take control of their health and wellbeing in revolutionary ways. But given America's patchwork data landscape of data privacy laws, how can users protect their privacy? Users should understand what their state requires in terms of data collection and handling, and they should read the privacy policies of period tracker apps. Companies like Consumer Report also provide helpful breakdowns of apps' privacy risks and things users should be aware of when choosing an app (Roberts 2022). Users should consider contacting their state representatives to express support for data privacy legislation because, particularly in a world that runs on data, legislators need to be paying attention to the ways that data can be misused. Digital platforms have revolutionized countless aspects of daily life, but they have simultaneously introduced new and unforeseen risks, and stricter regulation will be needed to protect people's health and safety.

REFERENCES

California Privacy Protection Agency. 2018. "California Consumer Privacy Act Of 2018." Cppa.ca.gov. 2018. https://cppa.ca.gov/regulations/pdf/cppa_act.pdf.

Conti-Cook, Cynthia. 2020. "Surveying the Digital Abortion Diary: A Preview of How Anti-Abortion Prosecutors Will Weaponize Commonly-Used Digital Devices as Criminal Evidence against Pregnant People and Abortion Providers in a Post-Roe America." SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3666305.

Dong, Zikan, Liu Wang, Hao Xie, Guoai Xu, and Haoyu Wang. 2022. "Privacy Analysis of Period Tracking Mobile Apps in the Post-Roe v. Wade Era." In Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering. New York, NY, USA: ACM.

Dresner, Stewart. 2024. "Blog - The EU GDPR May Be Open to Revision." Privacy Laws & Business. February 2024. https://www.privacylaws.com/reports-gateway/articles/int187/int187blog/.

Federal Trade Commission. 2013a. "Fair Credit Reporting Act." Federal Trade Commission.

July 19, 2013. https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

———. 2013b. "Children's Online Privacy Protection Rule ('COPPA')." Federal Trade Commission. July 25, 2013. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

Jillson, Elisa, and Miles Plant. 2021. "Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations That It Misled Consumers about the Disclosure of Their Health Data." Federal Trade Commission.

January 12, 2021. https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about.

Klosowski, Thorin. 2021. "The State of Consumer Data Privacy Laws in the US (and Why It Matters)." The New York Times, September 6, 2021. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

New America. 2024. "Enforcing a New Privacy Law." New America. 2024. https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/a-private-right-of-action-is-key-to-ensuring-that-consumers-have-their-own-avenue-for-redress/.

Roberts, Catherine. 2022. "Period Tracker Apps and Privacy." Consumer Reports. May 25, 2022. https://www.consumerreports.org/health/health-privacy/period-tracker-apps-privacy-a2278134145/.

U.S. Department of Education. 2021. "Family Educational Rights and Privacy Act (FERPA)." U.S. Department of Education. 2021. https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

Virginia Legislative Information System. 2024. "Code of Virginia Code - Chapter 53. Consumer Data Protection Act." Virginia.gov. 2024. https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/.

Wolford, Ben. 2018. "What Is GDPR, the EU's New Data Protection Law?" GDPR.Eu. November 7, 2018. https://gdpr.eu/what-is-gdpr/.

Wyden, Ron. 2021. "S.1265 - Fourth Amendment Is Not For Sale Act." Congress.gov. April 21, 2021. https://www.congress.gov/bill/117th-congress/senate-bill/1265/