

Data Privacy in the Femtech Industry

Every day, millions of women provide period-tracking apps such as *Clue* and *Flo* with intimate information about their bodies. In return, the apps offer algorithmic predictions that help users track, monitor, and improve their health. But is the convenience of these predictions worth the loss of privacy?

Smartphone apps like *Clue* and *Flo* are part of the larger “Femtech” industry. The term “Femtech” (short for “female health technology”) was coined in 2016 by Ida Tin, co-founder of *Clue*.¹ The industry is made up primarily of smartphone applications and wearable devices that track menstruation, fertility, and pregnancy.² In the past, these companies have been criticized for selling user data to marketing and analytics companies such as Facebook and Google.³ Recently, data privacy issues in the femtech industry received renewed attention following the U.S. Supreme Court’s decision to overturn *Roe v. Wade*, 410 U.S. 113 (1973). After a draft of *Dobbs v. Jackson Women’s Health Org.*, 142 S.Ct. 2228 (2022) was leaked, there were calls across social media for users of period-tracking apps to delete their data, as it could be used against them in states where abortion would soon be criminalized.⁴ 142 S.Ct. 2228 (2022).

Femtech companies operate outside the bounds of the Health Insurance Portability and Accountability Act (HIPAA).⁵ Users input the same information in the app as the information they share with their doctors; yet, information in the app is not subject to the same privacy requirements. Some states have legislation related to health data privacy, and companies are subject to the Federal Trade Commission’s prohibition against unfair and deceptive acts and practices.⁶ Yet, femtech companies are largely left unregulated on a federal level as it pertains to privacy and data security requirements for personal health information.⁷ Lacking an overarching privacy framework, femtech companies take a variety of approaches: some prioritize consumer privacy in device design and development, while for others, consumer privacy is an afterthought.⁸

¹ Ida Tin, *The Rise of a New Category: Femtech*, *Clue* (Sept. 14, 2016), <https://helloclue.com/articles/culture/rise-new-category-femtech>.

² See Celia Rosas, *The Future is Femtech: Privacy and Data Security Issues Surrounding Femtech Applications*, 15 *Hastings Bus. L.J.* 319, 320 (2019).

³ Alisha Haridasani Gupta & Natasha Singer, *Your App Knows You Got Your Period. Guess Who it Told?*, *N.Y. TIMES* (Jan. 28, 2021), <https://www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html>.

⁴ See Flora Garamvolgyi, *Why US Women are Deleting their Period Tracking Apps*, *THE GUARDIAN* (June 28, 2022).

⁵ Rosas, *supra* note 2, at 323.

⁶ Bethany Corbin, *The Shifting Data Privacy Landscape for Femtech & Beyond*, *MED DEVICE ONLINE* (June 29, 2022), <https://www.meddeviceonline.com/doc/the-shifting-data-privacy-landscape-for-femtech-beyond-0001>.

⁷ Rosas, *supra* note 2, at 323 (2019).

⁸ Corbin, *supra* note 6.

Lacking stronger regulation, users of these apps are left vulnerable to third parties who can their data against them. Today, many women are concerned that, in states where abortion has been criminalized, prosecutors will be able to subpoena information from their period-tracking phone apps as evidence. Other misuses of personal health data are foreseeable: spouses may be able to obtain personal health data from the apps during discovery in divorce proceedings, and insurance companies may be able to use personal health data to make determinations about whether or not to provide insurance to applicants. Even aside from these legal challenges, as a matter of principle, it is gravely concerning that companies professing to give women autonomy over their health are in fact selling off private, intimate data to the highest bidder.

Calls for action have come from many parties, ranging from social media users to the President himself. In an Executive Order signed on July 8, 2022, President Biden directed that the Secretary of Health and Human Services would “consider actions to educate consumers on how best to protect their health privacy and limit the collection and sharing of their sensitive health-related information.”⁹ Additionally, new apps such as *Stardust* have been launched, claiming to provide end-to-end encryption for all users.¹⁰

Mary Maas is from San Diego, California and is a second-year law student at Vanderbilt. She plans to practice litigation after graduation and spends much of her free time taking long strolls through Trader Joe’s and Target.

⁹ Exec. Order No. 14,076 (Protecting Access to Reproductive Healthcare Services).

¹⁰ Garamvolgyi, *supra* note 4.