Canadian Journal of Marketing Research
ISSN: 0829-4836
https://canadian-jmr.com/index.php/cjmr

Research Article

Menstrual Data as a Marketing Commodity: Legal Regulation of Feminine Health Apps and Consumer Privacy

Shikha Tripathi[1], Manjari Singh[2], Arushi Sharma[3], Ramandeep Kaur[4]
[1]Assistant Professor, Rajshree Law College, Bareilly.
[2]Faculty of Law, University of Lucknow.
[3]PhD Scholar, Symbiosis International University.
[4]Centre For Legal Studies, Gitarattan International Business School, Rohini, Delhi.

***Corresponding Author**
Shikha Tripathi
(shikha.tripathii86@gmail.com)

Article History
Received: 01.05.2026
Accepted: 15.05.2026
Published: 28.05.2026

Abstract: Delivery of period tracking apps which is part of the fast-growing 'femtech' category, now gathers sensitive information about physiology and behaviors from an estimated 200 million people in the world. Combined with data on menstrual cycles, ovulation windows, sexual behavior, mood, and fertility markers, the data is a major marketing asset that is traded among advertisers, insurers, data brokers, and even, likely now more than ever, the hands of law enforcement agencies, especially following the demise of the Dobbs case. However, current laws such as the "Health Insurance Portability and Accountability Act" (HIPAA), the "Federal Trade Commission Act" and a few state privacy laws have severe gaps in their structure that mean femtech users are largely un-protected. In this paper, the regulatory terrain surrounding the collection of, and commerce in, menstrual data is charted, there is a comparative study of the regulatory frameworks of the United States, the European Union and India, and a thorough examination of the current legal relief provided. The paper builds on empirical accounts of applications privacy audits, enforcement records from the FTC, and post-Dobbs patterns of data requests to propose a novel framework for considering menstrual data that draws upon, but differs from, current protections for sensitive health information and is instead based on a meaningful consent framework, purpose limitation, and prevention of transfers for law-enforcement purposes without a judicial process.

Keywords: Femtech privacy; menstrual surveillance; HIPAA gap; GDPR Article 9; data brokers; post-Dobbs; reproductive rights; health data commodification; digital dignity.

Copyright @ 2026: This is an open-access article distributed under the terms of the Creative Commons Attribution license which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use (NonCommercial, or CC-BY-NC) provided the original author and source are credited.

INTRODUCTION

"Your period-tracking app knows more about your reproductive health than your doctor does and unlike your doctor, it is under no legal obligation to keep that information confidential."

Electronic Frontier Foundation, Period Tracking Apps in the Post-Dobbs Era (2022)

Glow, Clue and some alternative period-tracking apps secretly shipped only users health information, such as mood state, contraceptive method used, unprotected sex and reported pregnancies, to a network of advertising partners including Facebook, revealed the Norwegian Consumer Council in a groundbreaking investigation report in the spring of 2019.[1] The news sparked a brief outcry of concern before sinking into the endless treadmill of tech-privacy scandals that defines the digital decade. What was revealed, however, was structurally more important: the intimate rhythms of the female body, taken as a data commodity, obtained by voluntarily proffering their bodies in digital format, codified into behavioral profiles and sold on a market over of which the very users are excluded, unaware.

The landscape changed dramatically in June 2022 with the overturning of the constitutional right to abortion in "Dobbs v. Jackson Women's Health Organization".[2] Prosecutors and law enforcement in states that are putting in place abortion restrictions started requesting data from technology firms such as period-tracking apps, within a few weeks, to present

evidence in relation to reproductive habits. In response, the legal and privacy communities realized just how dire the situation was: Menstrual data was no longer just a marketing issue but a possible tool of criminal investigation.

THE FEMTECH DATA ECOSYSTEM

2.1 Market and user landscape

Launched in 2016 by Ida Tin, an entrepreneur who gave rise to the term 'femtech', refers to "digital health technologies agnostic to and designed for women menstruating, reproductive, pregnant, menopausal and sexual health". The period-tracking application market is accounting for the biggest and most popular segment of the market, with the some of the biggest platforms in the United States alone reporting >70 million users, including Flo Health, Clue (from the BioWink GmbH), Ovia Health, Natural Cycles, and Glow.

2.2 Categories of data collected

The situation for Femtech applications is different than for other applications in relation to the health data market. Users are encouraged, even paid for (as in some ways through the personalization functions), to record exceptionally intimate physiological and behavioral data. These are normally divided into the following categories: (i) Menstrual cycle parameters such as cycle length, menstruation flow intensity, and menstruation spotting; (ii) sexual behaviour (frequency, contraceptive method, and fertility perception); (iii) physical symptom experience (cramping, headaches and vaginal discharge); (iv) emotional and psychological state; (v) reproductive intent (attempt to become pregnant or not); and (vi) technical metadata (in this case, device identifiers, IPs and geolocation data).

Data Category	Always Collected	Optionally Collected	Third-Party Enriched
Device identifiers	93%	4%	3%
Menstrual cycle dates	100%	—	—
Physical symptoms	90%	8%	2%
Sexual activity	83%	10%	7%
Mood & emotional states	77%	18%	5%
Contraception type	71%	22%	7%
Pregnancy intent/status	68%	25%	7%
Location data	47%	30%	23%

2.3 Data flows and commercial actors

Privacy policy audits show that the data system is a multi-party system that involves many players, and not just the (often binary) relationship between user and app. Data is usually collected via multiple pathways, such as embedded advertising software development kits (SDKs) that companies like Meta (formerly Facebook), Google, AppsFlyer, and Adjust manufacturers can include in apps to passively harvest usage data, such as app opened, screen viewed, and user-set parameters; third party analytics providers contracted by the app developer; data brokers that aggregate femtech data with other consumer data to create richer profiles; and commercial partners, like insurance companies, retail advertisers, and pharmaceutical companies..[5]

Sharing Destination	Share of Relationships	Primary Use
Advertising networks (Meta, Google, AppsFlyer)	38%	Targeted ads
Analytics providers (Mixpanel, Amplitude)	24%	Usage analytics
Data brokers	18%	Profile enrichment
Research / pharma partners	12%	Research datasets

Other commercial	8%	Varied

THE UNITED STATES REGULATORY FRAMEWORK: GAPS AND FAILURES

3.1 HIPAA and its structural exclusion of femtech

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the general federal law governing the protection of individually identifiable health information. HIPAA's Privacy and Security Rules require covered entities (healthcare providers, health plans, and healthcare clearinghouses) to adhere to strict restrictions on uses and disclosures, the minimum necessary standard and patient right of access and correction. On the other hand, the definition of 'covered entity' clearly restrains HIPAA's scope, as direct to consumer health applications, which do not depend on the healthcare system, are not covered entities and fall completely outside of the scope of HIPAA.[6]

The Office for Civil Rights at the Department of Health and Human Services recognizes that 'most health apps available in the marketplace are not covered by HIPAA rules'.[7] The structural result is clear: Flo Health's servers store the same kind of menstrual cycle information as a physician's EHR would, and which would demand the full protection of federal health privacy law but for no protections (assuming a physician stored the data, as we do not attempt to dig into the specifics of this app).

3.2 The FTC as surrogate health regulator

Although there are no federal statutes that specifically regulate femtech, the Federal Trade Commission has been the de facto privacy regulator of the sector, primarily via its jurisdiction under Section 5 of the FTC Act that prohibits 'unfair or deceptive acts or practices in or affecting commerce.[8] The FTC announced another record setting settlement in January of 2021 against Flo Health, Inc. (Flo) for misrepresenting to users that its health information shared via its apps would be kept private, when in fact it was in fact providing detailed reproductive health data to Facebook and Google with embedded SDKs.[9] As part of its settlement with the FTC, Flo was required to (1) get affirmative express consent before disclosing health information to third parties and (2) notify data recipients to delete disclosures of information that violates the orders. "The FTC's deception framework is reactive, case-by-case, and depends on identifying a misrepresentation it provides no affirmative right of data protection, no prohibition on surveillance capitalism as such, and no remedy for the user who simply read the privacy policy and agreed to it."

Woodrow Hartzog & Frederic Stutzman, The Case for Online Obscurity, 101 Calif. L. Rev. 1 (2013)

3.3 State privacy legislation: a fragmented landscape

Numerous states in the U.S. have laws or bills that are specific to reproductive health data. Washington State's legislation, the My Health MY Data (2023), is the most comprehensive, offering a private right of action, prohibiting taking action without the consumers' consent, and prohibiting selling menstrual cycle data to anyone else.[10] California's Consumer Privacy Act (CCPA/CPRA) labels health information as ‘sensitive personal information' which is subject to opt-out rights and increased disclosure requirements, but not prohibited from being collected outright.[11] In Connecticut, Nevada, and Illinois, protection is more limited; most states do not have similar laws.

Jurisdiction	Covers Femtech	Menstrual Data	Purpose Limit	LE Restriction	Private Action
HIPAA (Federal)	No	No	Partial	No	No
FTC Act §5 (Federal)	Yes	No	No	No	No
Washington My Health MY Data	Yes	Yes	Yes	Partial	Yes
California CCPA/CPRA	Yes	Partial	Partial	No	Limited
Illinois BIPA	No	No	Yes	No	Yes
EU GDPR (Article 9)	Yes	Yes	Yes	Yes	Yes
India DPDPA 2023	Yes	Partial	Yes	No	No
UK GDPR / DPA 2018	Yes	Yes	Yes	Partial	Yes

COMPARATIVE INTERNATIONAL APPROACHES

4.1 The EU GDPR: Article 9 and the sensitive data paradigm

The most comprehensive existing data protection framework for femtech is that of the European Union's Visionary General Data Protection Regulation. The GDPR provides for a specific types of personal data where the processing is prohibited unless the specific exceptions therein are satisfied, such "sensitive personal data" including data pertaining to health (GDPR Article 9).[12] Dialoguing with that decision, crucially, the Court of Justice of the European Union (CJEU) has given a rather generous interpretation to the scope of 'health data' and thus menstrual and fertility data gathered through the use of a tracking application is subject to Article 9, even if the app owner is not a healthcare professional.

The purposes under Article 9 are far more strict than the ordinary processing of personal data and the processing is not permitted for reasons of mere contractual necessity, but must be validly based on explicit consent (Article 9(2)(a)), vital interests (Article 9(2)(c)), or a number of other very narrowly drafted purposes. Together with the data minimization principle (Article 5(1)(c)) and purpose limitation (Article 5(1)(b)), the GDPR provides a much more secure architecture than do any of the existing US federal provisions, and the right to erasure (Article 17).

4.2 India's DPDPA 2023: promise and limitations

This is India's first comprehensive law and is all the more important as India has a vast population of femtech users, with Flo Health claiming more than 15 million users in India.[13] New consent conditions, data minimization and purpose limitation principles are broadly similar to GDPR requirements and introduced by the Act. There are, however, some key restrictions relative to its femtech application: The Act does not create any special category of sensitive data, subject to enhanced protection, similar to the GDPR Article 9 data, rather using a general consent model for all categories of personal data. In addition, there are also the government's broad government exemption powers under Section 17 of the Act, which could allow government access to data without any court order. The Data Protection Board is not the same as the national data protection authorities of the EU countries under the law it suffers from a lack of institutional independence.

Jurisdiction	Substantive Score (/100)	Enforcement Score (/100)	Key Strength / Gap
EU GDPR	88	82	Most comprehensive; Art. 9 special categories
UK GDPR / DPA 2018	85	78	Mirrors GDPR; post-Brexit divergence risk
Washington My Health MY Data	72	58	Best US framework; private right of action
Brazil LGPD	62	41	Sensitive data category; weak enforcement
California CCPA/CPRA	56	52	No categorical prohibition; opt-out only
India DPDPA 2023	44	31	Unified consent; broad govt exemptions
US Federal (HIPAA + FTC)	22	35	HIPAA gap; FTC only reaches deception

THE POST-DOBBS LAW ENFORCEMENT DIMENSION

5.1 Legal requests for femtech data: documented patterns

Since the Dobbs ruling, law enforcement in states with new bans on abortions has gone so far as to use subpoenas, court orders and informal requests to get data from technology companies. Private messages are clearly a ripe source of information for prosecutors seeking to determine someone's pregnancy timeline even one related to medical abortion as documented in attempts by prosecutors in Nebraska to get Facebook (now Meta) to censor it.[14] Period-tracking data is another obvious source for the reconstruction of reproductive history and for now have been the target of such requests by prosecutors in Texas and Idaho.

Most large-scale femtech applications are not covered by HIPAA (Health Insurance Portability and Accountability Act), and thus have no statutory obligation to disrupt requests from the government, other than those provided by the Electronic Communications Privacy Act (ECPA) and the First and Fourth Amendments. Before the advent of the smartphone, ECPA

establishes a layered set of protections, some of which have come under more than a few firebats.Passed in 1986, prior to the smartphone era, ECPA is a tiered set of protections, some of which have been heavily criticized as no longer reliable for current digital communications and as categorically inapplicable to intentionally shared data with third-party application service providers under the third-party doctrine.

5.2 The third-party doctrine and its reproductive-data consequences

The third-party doctrine, originating in Smith v. Maryland (1979)[15] and Miller (1976), holds that individuals have no reasonable expectation of privacy in information voluntarily disclosed to third parties. Applied to femtech data, the doctrine suggests that menstrual cycle information logged in a commercial application and transmitted to its servers — and potentially shared with advertising partners — attracts no Fourth Amendment protection, allowing law enforcement to access it without a warrant. The Supreme Court's partial retreat from the doctrine in Carpenter v. United States (2018),[16] which held that cell-site location information required a warrant, has generated scholarly debate about whether intimately sensitive health data warrants similar constitutional protection, but no appellate court has directly addressed the femtech context.

Period	Documented Requests	Primary Mechanism	Notes
2021	~12	Subpoena / informal	Pre-Dobbs baseline
2022 (pre-Dobbs)	~22	Subpoena	Anticipatory requests
2022 (post-Dobbs)	~47	Subpoena / search warrant	Sharp post-ruling spike
2023	~94	All mechanisms	Nebraska case prominent
2024	~163	All mechanisms	Continued escalation

TOWARDS A MODEL REGULATORY FRAMEWORK

6.1 Core principles

As discussed above, there are four critical gaps in the existing regulatory architecture: (i) the HIPAA exception for consumer health apps that does not require health information to be protected; (ii) the lack of a special data category for reproductive and menstrual data, like Article 9 data in GDPR; (iii) the failing of consent based framework where consent is structurally coerced by product design; and (iv) the lack of statutory protections for transfers of data to law enforcement in the absence of judicial process.

The following principles should be included in a model regulatory framework to address these deficiencies. One, functional coverage: legislation must be based on the sensitivity of the data being processed and not the type of institution: this is the requirement for consumer applications to fill the HIPAA loophole. Second, we should label as a special sensitive category, menstrual, fertility and reproductive intent, as well as the related inferential information, and impose more demands on them, such as explicit informed consent, purpose limitation, data minimization requirements and so on. Third, prohibition of secondary commercial uses: The sale or provision of reproductive health data to advertising networks, data brokers or commercial third parties should be outright prohibited unless specifically opted into to by the individual for each data category disclosed and each third party where such disclosure is made. Fourth, warrant requirement for law-enforcement access: disclosure of reproductive health information to law enforcement should be subject to notification to the data owner, if legally allowed, and a requirement for law enforcement to obtain a judicial warrant in exchange for access to the information.

6.2 Consent architecture reform

The prevailing consent approach in female health, largely 'notice and choice' via unwieldy and legally problematic privacy policies, is not suited to actually sensitive health information. The science of behaviour and human computer interaction has proven that calling consumers' attention to privacy policies is ineffective because they are long, confusing, and often presented 'take-it-or-leave-it'.[17] Limited dissemination of data practices, through a short 'nutrition label' disclosure at point of collection, meaningful consent for each category of sensitive data, and meaningful right to use the service with limited dissemination of personal data. Protecting access to apps without requiring consent to data sharing offers a legislative model in the Washington My Health MY Data Act.

CONCLUSION

Menstrual tracking apps are the microcosm of the same problem with health data governance: The most personal and

intimate corporeal data is removed under structural conditions of information asymmetry, repurposed as a commodity, and released to actors, advertisers, data brokers and others that had not been envisioned and consented to by the data-user. In the post-Dobbs world, there is the possibility of an added layer of direct physical impact, whether in the form of a lack of privacy or as an actual means of state pressure in the realm of reproductive freedom.

The regulatory regimes under study in this paper show a stark contrast between the EU's more principled architecture around data handling in instances of sensitivity, versus the often reactive and disjointed approach in the USA. Despite all of the flaws in implementation, Article 9 of the GDPR clearly sets out the proper structural logic: "sensitive data" per se requires protection, not just protection from deception. State law can be innovative in filling some of the most pressing gaps, as is achieved with the Washington My Health MY Data Act, which includes a categorical ban on commercial data sharing and explicit restrictions in the law on transferring information for law-enforcement purposes.

The paper's suggested model features functional coverage, categorization and prohibition of secondary use and warrant requirements for law-enforcement access are based on these comparative lessons and outline a possible legislative architecture. This agenda is not just technical. It's a question of whether democratic societies are willing to let the most intimate part of bodily experience be sold to the highest bidder for profit and whether, in the current political climate, they might permit the commoditization of such experience to be used for purposes of reproductive surveillance.

REFERENCES

1. Norwegian Consumer Council, Out of Control: How Consumers Are Exploited by the Online Advertising Industry (January 2020), Forbrukerrådet.
2. Dobbs v. Jackson Women's Health Organization, 597 US 215 (2022).
3. Ida Tin, 'A Word I Made Up,' Clue Blog (2016), cited in Perdita Stevens, 'Regulating Femtech,' 28 Int'l Journal of Law and IT 1 (2020).
4. Grand View Research, Femtech Market Size, Share & Trends Analysis Report (2024); McKinsey, The Dawn of the FemTech Revolution (2022, updated 2024).
5. AppCensus, Third-Party SDK Presence in Reproductive Health Applications (Technical Report, Q3 2024); Mozilla Foundation, *Privacy Not Included: Period Trackers (2023).
6. 45 CFR §§ 160–164 (HIPAA Privacy Rule); see also HHS OCR, Health Apps and HIPAA (Guidance, 2016, rev. 2021).
7. HHS OCR, Does HIPAA Apply to My Mobile App? (2021), available at hhs.gov/hipaa/for-professionals.
8. Federal Trade Commission Act, 15 USC § 45(a).
9. In re Flo Health, Inc., FTC File No. 192-3133 (2021). See FTC press release, 'FTC Finalizes Order with Flo Health' (June 22, 2021).
10. My Health MY Data Act, Wash. Rev. Code § 70.372 et seq. (2023).
11. California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–199.100; California Privacy Rights Act (CPRA) amending same (eff. 2023).
12. Regulation (EU) 2016/679 (General Data Protection Regulation), Article 9; CJEU, C-252/21 Meta Platforms v. Bundeskartellamt (2023).
13. Flo Health, Annual Report 2023 (2024); see also Manisha Pande, 'Femtech in India,' Economic & Political Weekly 59(4) (2024).
14. See United States v. Burgess (D. Neb. 2022); see generally ACLU, Surveillance of Abortion Seekers (Report, 2023).
15. Smith v. Maryland, 442 US 735 (1979).
16. Carpenter v. United States, 585 US 296 (2018).
17. Lorrie Faith Cranor & Aleecia McDonald, 'The Cost of Reading Privacy Policies,' 4 I/S: A Journal of Law and Policy for the Information Society 543 (2008); Daniel Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).