Institute for Youth in Policy

5214F Diamond Heights Blvd #3055
San Francisco, CA 94109
+1 (715) 469-6884
fellowship@yipinstitute.org
www.yipinstitute.org/fellowship/

Fellowship Capstone | Policy Brief

My Body, My Data: Exploring Reproductive Health Data Privacy in Post-Roe America

Ellyce Butuyan

I. Executive summary

Reproductive health data privacy has become a pressing concern in post-Roe America, where the reversal of federal abortion protections has intensified state-level surveillance and legal risks. As digital footprints, from period tracking apps to search histories, have the potential to be weaponized, the need for strong and standardized data privacy protections has never been more urgent. This brief will examine how targeted policy measures can safeguard reproductive digital privacy in a rapidly shifting technological and legal landscape.

II. Overview

In recent years, the concern of technological privacy, especially concerning reproductive health data privacy has arisen. Despite past progress and precedent that has protected the women's right to choose, landmark Supreme Court Decisions, new presidential administrations, and the innovation of technology and biometric data has challenged the ideological individual liberties of abortion. Therefore, this paper explores the ever fluctuating intersection of policy, technology, and social inequality in order to propose new changes to current legislation that will protect individual rights and bodily autonomy within the world of reproductive health.

A. Relevance

Protected health information (PHI) refers to any data within a medical or designated record set that can be linked to a specific individual and is generated, utilized, or shared during the delivery of healthcare services like diagnosis or treatment. The rapid evolution of technology such as the rise of Femtech and big data analytics through consumer apps and websites that are not considered entities covered by HIPAA has intensified privacy risks regarding the PHI of consumers. Oftentimes, the complexity of these systems and the fragmented regulatory landscape leave individuals vulnerable to exploitation and loss of control over their PHI. This opacity can lead to unauthorized data collection, invasive surveillance, and the erosion of individual autonomy, particularly as Big Tech companies aggregate and analyze data across multiple platforms.

III. History

A. Current Stances

The bodily autonomy of women has been a contested subject throughout global history, and this tension is reflected in the United States through the multifaceted barriers to abortion access, including logistical challenges, financial hurdles, and complex state regulations. Prior to 1973, abortion in the United States was largely

illegal and highly stigmatized. In the late 1800s, a wave of criminalization led by the American Medical Association and reinforced by religious groups resulted in abortion being outlawed in every state by 1910, except in rare cases to save a woman's life. By the 1960s and early 1970s, some states began to reform or repeal these strict bans, often allowing abortion in cases of rape, incest, or threats to a woman's physical or mental health. The 1973 Supreme Court Case Roe v. Wade recgonized that the right to abortion was protected by the 14th Amendment as it is an individual right and liberty. The number of abortions in the U.S. increased for several years, peaking in the late 1980s and early 1990s, based on data from both the CDC and the Guttmacher Institute. Since that peak, the overall number of abortions has gradually declined.

The U.S. Supreme Court broke more than 50 years of precedent after overturning Roe v. Wade in Dobbs v. Jackson Women's Health Organization in 2022, resulting in the loss of abortion as a federal constituional right and leaving states to decide their own regulations for abortion. Consequently, the reproductive health data for women is now at risk in regions where abortion is illegal or not protected. Pre-Dobbs, around 37% of women in states like Arizona, Iowa, New Jersey, Ohio, and Wisconsin used period/fertility-tracking apps. Post-Dobbs, usage increased to 45% in these states, driven by heightened awareness of pregnancy timing amid abortion restrictions. More users present more risks for unjust penalization and the intrusion on PHI. This presents a dangerous tradeoff for women today who are navigating the complexities of using such technologies, with apps like Flo and Clue reporting 40 million and 11 million monthly active users, respectively.

IV. Policy Problem

A. Stakeholders

Central to the issue are women and individuals seeking reproductive health care or using digital health tools such as period and fertility tracking apps. These individuals face heightened risks in the current legal landscape, where their personal health data can be accessed or weaponized by authorities in states with restrictive abortion laws. As a result, their autonomy and privacy are threatened, leaving them vulnerable to surveillance, prosecution, or discrimination based on their reproductive choices. Ideally, these women and individuals should have a decisive stake in the policies governing the collection, use, and sharing of their health data, ensuring that such mechanisms are protective, transparent, and just.

Healthcare providers are also central stakeholders, as they are entrusted with safeguarding patient confidentiality while navigating a patchwork of state and federal regulations. The shifting legal environment places providers in a precarious position, potentially exposing them to legal liability for simply delivering care or maintaining patient privacy. Therefore, it is essential that providers are included in policy discussions and that clear guidelines are established to protect both their professional responsibilities and their patients' rights.

Technology companies and app developers stand

to play a pivotal role as custodians of vast amounts of sensitive reproductive health data. However, the lack of comprehensive regulation means these companies often operate in a gray area, with inconsistent privacy practices that can leave users exposed. It is crucial to hold these companies accountable and to encourage the adoption of robust, standardized privacy protections that prioritize user consent and security.

Government agencies and law enforcement are stakeholders as both regulators and potential data requestors. In states with restrictive abortion laws, law enforcement may seek access to reproductive health data for investigations, raising profound concerns about the misuse of personal information. Policymakers at both the state and federal levels must recognize the gravity of these risks and work to enact clear, enforceable privacy standards that safeguard individual rights.

Finally, third-party data brokers and commercial entities are stakeholders due to their ability to aggregate and monetize reproductive health data, often without the knowledge or consent of the individuals involved. This underscores the urgent need for comprehensive data privacy legislation that addresses not only direct data collectors but also the broader ecosystem of data sharing and commercialization.

B. Risks of Indifference

Failing to effectively protect reproductive health data privacy can result in serious consequences, including the misuse of sensitive personal information, increased surveillance or targeting of individuals seeking reproductive care, loss of trust in healthcare providers and digital platforms, and potential legal or social repercussions for patients in states with restrictive reproductive health laws.

C. Nonpartisan Reasoning

Protecting reproductive health data is a nonpartisan issue with broad societal implications. The rationale for safeguarding this sensitive information can be structured as follows:

1) Protection of Individual Liberty and Autonomy

Reproductive health data often contains some of the most personal and intimate details about an individual's life. Ensuring its privacy is fundamental to upholding personal autonomy and freedom from unwarranted surveillance or interference. Without strong protections, individuals may fear seeking necessary healthcare or using digital tools, undermining their ability to make informed decisions about their own bodies.

2) Public Health and Continuity of Care

When patients worry that their reproductive health data could be exposed or misused-especially across state lines where laws differ-they may withhold information or avoid care altogether. This reluctance can disrupt continuity of care, leading to poorer health outcomes, delayed diagnoses, and increased public health risks. Protecting data privacy encourages open communication between patients and providers, which is essential for effective and safe healthcare delivery.

3) Economic and Societal Stability

Breaches of reproductive health privacy in states with restrictive abortion laws or limited reproductive rights can result in job loss, discrimination, or legal jeopardy, particularly in environments where reproductive choices are criminalized or stigmatized. Such risks can destabilize households and communities, affecting workforce participation and economic productivity. By protecting this data, society helps ensure that individuals can participate fully and safely in economic and civic life, benefiting the broader economy and community resilience.

4) Legal and Ethical Compliance

Inconsistent privacy protections across jurisdictions create legal uncertainty for both patients and providers. Clear and robust data protections help organizations comply with evolving laws, reduce the risk of inadvertent legal exposure, and support ethical standards in healthcare and technology. Nonpartisan policies that safeguard reproductive health data help maintain the integrity of medical practice and uphold democratic values of fairness and justice.

V. Tried Policy

The landmark piece of legislation addressing PHI was established in 1996: The Health Insurance Portability and Accountability Act (HIPPA). HIPPAA established national standards to protect medical records and PHI and gave individuals rights over their protected health information.

In 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH) was passed to promote the adoption and meaningful use of health information technology. In addition to encouraging electronic health record (EHR) adoption, HITECH strengthened HIPAA privacy and security rules, making business associates directly liable and increasing penalties for violations and required notification of individuals and authorities in the event of data breaches involving protected health information. However, the HITECH Act presented ongoing privacy and security risks as digital records introduced new cybersecurity challenges that many struggled to address.

After Roe v. Wade was overturned in 2022, the Biden Administration passed the HIPPA Privacy Rule to Support Reproductive Healthcare Privacy, prohibiting covered entities from disclosing protected health information (PHI) for the purposes of imposing criminal, civil or administrative liability on a person who is obtaining or providing legal reproductive healthcare. However, the rule has been met with numerous legal challenges, making its future uncertain. In September 2024, Texas Attorney General Ken Paxton sued HHS over the rule, alleging that it unlawfully prevents states from using their investigative authority. In January 2025, just days before President Trump took office, 15 states joined the Texas lawsuit to challenge the rule. They argued that the final rule would hinder their ability to collect vital information needed to investigate serious misconduct, including Medicaid billing fraud, child and elder abuse, and insurance-related

violations. In addition to this uncertain legal landscape, the new rule also fails to extend to the majority of reproductive healthcare apps; 84% of period-tracking apps have sold data to third parties without users' consent, and 64% are required to share data with law enforcement if subpoenaed, which is particularly concerning post-Roe.

VI. Policy Options

Standardization of Digital Health Data Practices

The lack of consistent standards for collecting, storing, and sharing reproductive health data-especially among apps and non-HIPAA-covered entities-creates vulnerabilities and confusion for both users and providers. Therefore, it is necessary to implement a federal framework that mandates standardized, transparent data handling practices for all entities managing reproductive health data, including mobile apps and tech companies. This framework should include clear consent protocols, data minimization requirements, and regular third-party audits. Oversight could be provided by an independent body such as the Federal Trade Commission (FTC) or a newly established Office for Digital Health Privacy.

Comprehensive Consumer Data Privacy Legislation

Current privacy protections (HIPAA, HITECH) do not cover most consumer health apps, leaving a significant gap in user protection. I propose amending these policies to consider mobile health apps, wearable devices, and data brokers, as HIPPA covered entities and enacting a federal consumer data privacy law specifically addressing health-related data outside traditional healthcare settings (such as data stored within Femtech databases). This law should require explicit, informed consent for data collection and sharing, prohibit the sale or sharing of reproductive health data without user permission, provide individuals with the right to access, correct, and delete their data, and impose strict penalties for unauthorized disclosures or breaches.

Public Awareness and Digital Literacy Campaigns

Users often lack awareness of how their reproductive health data is collected, used, or shared, leading to uninformed consent and increased risk. Currently, the 2024-2030 Federal Health IT Strategic Plan is being developed and implemented by the U.S. Department of Health and Human Services (HHS) in collaboration with more than 25 federal agencies. This specific federal policy framework prioritizes the ethical and equitable design, implementation, and secure, private use of health IT to effectively serve all populations. The current framework does not include specific guidelines and information regarding reproductive health privacy. Thus, it is critical that future iterations of the plan explicitly address the unique risks associated with reproductive health data, particularly in the context of Femtech applications and evolving state laws, to ensure comprehensive protections for all users.

VII. Conclusions

In this brief, I have examined the urgent challenges surrounding reproductive health data privacy in post-Roe America, highlighting the vulnerabilities created by technological

innovation, fragmented regulation, and shifting legal landscapes. Through an analysis of historical context, current policy gaps, and the heightened risks faced by individuals and providers, it is clear that the status quo leaves too many exposed to potential harm and loss of autonomy. Of the policy options explored, the most actionable and far-reaching are the implementation of comprehensive consumer data privacy legislation and the standardization of digital health data practices, which together would close critical loopholes and extend protections beyond traditional healthcare settings.

However, true progress requires not only regulatory reform but also a concerted effort to empower individuals through public awareness and digital literacy. As technology continues to outpace policy, it is essential that future federal strategies-such as the Federal Health IT Strategic Plan-explicitly address the unique risks of reproductive health data and prioritize the needs of those most affected. Achieving meaningful privacy protections will demand sustained attention, cross-sector collaboration, and a pragmatic commitment to upholding individual rights in a rapidly evolving digital world. By systematically advancing these solutions, we can move toward a future where reproductive health data is safeguarded, trust in technology is restored, and personal autonomy is respected for all.

Acknowledgment

The Institute for Youth in Policy wishes to acknowledge Taylor Beljon-Regen, Alexis Kagan, Brinkley Bennett, Asher Cohen and other contributors for developing and maintaining the Fellowship Program within the Institute.

References

[1] Abortion laws by state. (n.d.). Center for Reproductive Rights. https://reproductiverights.org/maps/abortion-laws-by-state/

[2] Before Roe v. Wade: Women reflect on what life was like. (n.d.). PBS NewsHour. https://www.pbs.org/newshour/show/women-reflect-on-what-life-was-like-before-roe-v-wade#:~:text=Before%20the%201973%20Supreme%20Court,tried%20to%20induce%20abortions%20themselves.

[3] Doctorsoftheworld.org. (n.d.). Project 2025: Sexual and reproductive health rights. https://doctorsoftheworld.org/blog/project-2025-sexual-and-reproductive-health-rights/

[4] Federal Register. (2024, April 26). HIPAA Privacy Rule to Support Reproductive Health Care Privacy. https://www.federalregister.gov/documents/2024/04/26/2024-08503/hipaa-privacy-rule-to-support-reproductive-health-care-privacy

[5] FTC finalizes order: Flo Health fertility tracking app shared sensitive health data with Facebook, Google. (2021, June). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google

[6] Guttmacher Institute. (2025, March). With risks to patients and providers growing, states should revisit abortion reporting requirements. https://www.guttmacher.org/2025/03/risks-patients-and-providers-growing-states-should-revisit

-abortion-reporting-requirements

[7] HIPAA Privacy Rule Final Rule to Support Reproductive Health Care Privacy: Fact Sheet. (n.d.). U.S. Department of Health & Human Services. https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/final-rule-fact-sheet/index.html

[8] HIPAA Privacy Rule. (n.d.). U.S. Department of Health & Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html#:~:text=The%20HIPAA%20Privacy%20Rule%20establishes,care%20providers%20that%20conduct%20certain

[9] HITECH Act Enforcement Interim Final Rule. (n.d.). U.S. Department of Health & Human Services. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

[10] IAPP. (2025). The state of US reproductive privacy in 2025: Trends and operational considerations. https://iapp.org/news/a/the-state-of-us-reproductive-privacy-in-2025-trends-and-operational-considerations

[11] IAPP. (n.d.). Privacy and digital health data: The femtech challenge. https://iapp.org/news/a/privacy-and-digital-health-data-the-femtech-challenge

[12] LSE Human Rights Blog. (2022, December 14). Rethinking explicit consent and intimate data collection: The looming digital privacy concern with Roe v. Wade overturned. https://blogs.lse.ac.uk/humanrights/2022/12/14/rethinking-explicit-consent-and-intimate-data-collection-the-looming-digital-privacy-concern-with-roe-v-wade-overturned/

[13] My Health, My Data Act: Protecting Washingtonians' personal health data and privacy. (n.d.). Washington State Office of the Attorney General. https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy

[14] Navigating HIPAA's reproductive healthcare data privacy rule. (n.d.). TechTarget. https://www.techtarget.com/healthtechsecurity/feature/Navigating-HIPAAs-reproductive-healthcare-data-privacy-rule

[15] Paubox. (n.d.). The hidden vulnerabilities in sharing reproductive health information. https://www.paubox.com/blog/the-hidden-vulnerabilities-in-sharing-reproductive-health-information

[16] Period apps after Dobbs: More users, more risks. (n.d.). Public Health Post. https://publichealthpost.org/sexual-reproductive-health/period-apps-after-dobbs-more-users-more-risks/

[17] Pew Research Center. (2024, March 25). What the data says about abortion in the US. https://www.pewresearch.org/short-reads/2024/03/25/what-the-data-says-about-abortion-in-the-us/

[18] Reproductive Rights. (n.d.). Roe v. Wade. https://reproductiverights.org/roe-v-wade/

[19] Reproductive Rights. (n.d.). Supreme Court takes away right to abortion. http://reproductiverights.org/supreme-court-takes-away-right-to-abortion/

[20] ScienceDirect. (2023). [Article on reproductive health privacy]. https://www.sciencedirect.com/science/article/pii/S1472648323006983

[21] Supreme Court of the United States. (1992). Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833. https://supreme.justia.com/cases/federal/us/505/

833/

[22] UC Berkeley Committee for Protection of Human Subjects. (n.d.). What is PHI? https://cphs.berkeley.edu/hipaa/hipaa18.html#:~:text=What%20is%20PHI%3F,such%20as%20diagnosis%20or%20treatment.