Arizona Law Journal of Emerging Technologies

Volume 8 *Article 1*

1-2024

HER DATA, HER CHOICE: A COMPREHENSIVE LOOK AT FEMTECH PRIVACY CONCERNS

Violet Konopka
University of Arizona James E. Rogers College of Law

2024-2025 https://azlawjet.com Vol. 8, Art. 1

Arizona Law Journal of Emerging Technologies

Her Data, Her Choice: A Comprehensive Look at Femtech Privacy Concerns

Violet Konopka, J.D Candidate 2024

Table of Contents

HER DATA, HER CHOICE: A COMPREHENSIVE LOOK AT FEMTECH PRIVACY CONCERNS

Violet Konopka

I. Abstract

The land of the free? Americans today feel that they have very little, or even no control over their data being collected by private companies and the government.[1] A huge majority of Americans are also concerned about how the data collected is being used. Women are—and should be[2]—especially wary of the data they share, particularly when it comes to menstrual data.[3] With the recent *Dobbs* decision by the Supreme Court of the United States, data protection has never been more important to preserving reproductive access for women across the country. This decision ended the constitutional right to an abortion and left the states to make their own policies regarding reproductive health. Now that this is the case, it is especially important that women's health data be kept private to avoid prosecution. This Note explores the common uses and avenues by which health data is collected by women, current regulations in place to protect this data, and where policy changes can be made to provide better protection.

II. Introduction

The digital health industry has experienced a huge boom over the past couple of years with more than 100,000 health applications available for smartphones.[4] Digital health technologies specifically tailored to women, also known as *Femtech*, have been no exception with funding reaching nearly $2.5 billion in December 2021.[5] A large majority of the consumer solutions in this arena focus on menstrual, gynecological, pelvic, and sexual health.[6] The most potentially worrisome forms of Femtech in this post-*Dobbs* age are fertility tracking apps (FTAs) and wearable devices. Although users

[1] 81% of Americans believe they have very little/no control over the data companies collect and 84% believe the same for data collected by the government. Brook Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling -lack-of-control-over-their-personal-information/.

[2] Although this is not always the case, for the sake of clarity, "women" will be used throughout this note to denote all people with uteri.

[3] Susan Hogan et al., *Why the Overturning of* Roe v. Wade *Has Some Women Deleting Fertility Treating Apps*, NBC WASH. (Aug. 25, 2022, 7:39 PM), https://www.nbcwashington.com/news/consumer/why-the-overturning-of-roe-v-wade-has-some-women-deleting-fertility-apps/3142328/.

[4] Charles JT Butcher & Wajid Hussain, *Digital Healthcare: The Future*, 9 FUTURE HEALTHCARE J. 113, 114 (2022).

[5] *The Dawn of the FemTech Revolution*, MCKINSEY & CO. (Feb. 14, 2022), https://www.mckinsey.com/industries/healthcare/our-insights/the-dawn-of-the-femtech-revolution.

[6] *Id.*

often assume that the data collected on these devices is covered by the Health Insurance Portability and Accountability Act (HIPAA),[7] this is the case in very few circumstances. But why are women using these apps? A study published in 2018 determined that women using FTAs had four main motivations: (1) to observe their menstrual cycle; (2) to conceive; (3) to inform fertility treatment; and (4) as contraception.[8] Women can track their cycles in a less intrusive manner, experience a greater sense of autonomy, and have greater accessibility to important resources when using FTAs.[9] By providing women with an opportunity to track their cycles, FTAs provide an alternative contraceptive option that is non-hormonal and less physically intrusive than the other top contenders.[10] The greater sense of autonomy also goes with improved self-worth which, of course, is incredibly important to an individual's mental health.[11]

Perhaps the most important benefit of these FTAs though is the accessibility they provide. Fertility education and access to a women's health care provider is not available for many women.[12] The women most directly impacted by this inaccessibility are often women of color and women from economically disadvantaged backgrounds. Since these women are disproportionately impacted by unintended pregnancies, access—and efficacy—is especially vital for their health.[13] In addition to being accessible, some FTAs are even specifically tailored to different cultural sensitivities.[14]

In early 1973, in *Roe v. Wade*, the Supreme Court decided that state abortion bans violated the Fourteenth Amendment and required a strict scrutiny analysis.[15] The Court reaffirmed this decision almost twenty years later in *Casey,* holding that women have the right to have an abortion without undue interference from the government.[16] The *Dobbs* decision, which was issued in June 2022, overturned these cases and held that a right to abortion was not provided by the federal Constitution, so the authority to regulate abortion must be left to the states.[17]

Even before this decision came down, thirteen states had passed "trigger laws" that would put an almost immediate ban on abortions if and when the Supreme Court

---

[7] Tawanna Lee & Antonio Reynolds, *All Data Is Not HIPAA Data – Healthcare Covered Entities Should Pay Close Attention to State Privacy Laws Regulation the Health IoT Ecosystem*, JD SUPRA (July 13, 2021), https://www.jdsupra.com/legalnews/all-data-is-not-hipaa-data-healthcare-3523068/.
[8] Kate Gambier-Ross et al., *A Mixed Methods Exploratory Study of Women's Relationships with and Uses of Fertility Tracking Apps*, 4 DIGIT. HEALTH 1, 1 (2018).
[9] Alexandra M. Taylor, Note, *Fertile Ground: Rethinking Regulatory Standards for Femtech*, 54 U.C. DAVIS L. REV. 2267, 2296–97 (2021).
[10] *See id.* at 2289.
[11] *Id.* at 2297.
[12] *Id.*
[13] *Id.*
[14] For example, *Health in Her HUE* for black women and *FOLX Health* for LGBTQ+ populations. *The Dawn of the FemTech Revolution, supra* note 5, at 5.
[15] Roe v. Wade, 410 U.S. 113, 164 (1973).
[16] Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833, 846 (1992).
[17] Dobbs v. Jackson Women's Health Org., 597 U.S. 215, 292 (2022).

overturned the federal right to abortion access established in *Roe*.[18] As of April 9, 2024, twenty-one states have either entirely banned abortion or enacted a ban more restrictive than permitted under *Roe*.[19] That means that women in almost half the states now have less access to reproductive health care than women have had for the past nearly 50 years. It is now more important than ever for women's reproductive health data to be accurate and secure.

III. So What?

What is *privacy*? There is not exactly a straight-forward answer to this question. The International Association of Privacy Professionals broadly defines privacy as "the right to be let alone, or freedom from interference or intrusion."[20] Data privacy is a bit more specific and relates to a person's right to keep their individual information from unauthorized access.[21] Many organizations, including the federal government,[22] the International Covenant on Civil and Political Rights,[23] and the European Union,[24] all agree that privacy is important. But why is that the case? Some reasons cited as the foundation for privacy protection include the assurance of human dignity, the ability for individuals to retain autonomy, and a necessary part of other rights like freedom of expression, religion, and association.[25] So, when this privacy is violated, there are a whole host of harms that can arise, including reputational damage, discrimination, emotional distress, weakened sense of self, and much more.[26] Even beyond the individual level, privacy serves society as a whole. When people feel that their information is being kept private, they are more willing to share their data with researchers, making way for more representative and holistic research to be performed.[27]

Unfortunately, data is not always kept as private as many consumers may prefer or believe it to be. Most organizations that acquire user data have a privacy policy that users must agree to before using their services. However, a study conducted in 2019 showed that less than ten percent of Americans always read these policies before

[18] Jesus Jimenez, *What Is a Trigger Law? And Which States Have Them?,* N.Y. TIMES (May 4, 2022), https://www.nytimes.com/2022/05/04/us/abortion-trigger-laws.html.
[19] Allison McCann & Amy Schoenfield Walker, *Tracking Abortion Bans Across the Country*, N.Y. TIMES, https://www.nytimes.com/interactive/2024/us/abortion-laws-roe-v-wade.html?searchResultPosition=3 (Aug. 13, 2024, 3:51 PM).
[20] *What Does Privacy Mean?*, IAPP, https://iapp.org/about/what-is-privacy/ (last visited Aug. 15, 2024).
[21] Donal Tobin, *What Is Data Privacy-and Why Is It Important?*, INTEGRATE.IO (Feb. 22, 2024), https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important/.
[22] NAT'L INST. OF HEALTH, BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 75–110 (Sharyl J. Nass et al., eds., 2009).
[23] *The Importance of Privacy*, OVIC, https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-officer-toolkit/the-importance-of-privacy/ (last visited Aug. 15, 2024).
[24] *European Union – Data Privacy and Protection,* INT'L TRADE ADMIN., https://www.trade.gov/european-union-data-privacy-and-protection (last visited Aug. 15, 2024).
[25] *The importance of privacy*, *supra* note 23.
[26] *Id.*
[27] *See* NAT'L INST. OF HEALTH, *supra* note 22, at 83–86.

agreeing to them, and even less actually understand what it is that they are agreeing to.[28] Even the rare users who actually read and understand the policy have no real power, as they cannot negotiate their own terms and instead, have to agree or forgo the service the company may be providing.[29] Of course, this could be as simple as not being able to play an online game with friends. But it could also be as detrimental as being unable to track important health data.

Much of the health data being shared is highly sensitive, potentially embarrassing, and can directly harm individuals if it is not kept private.[30] Some health information could, if made public, cause individuals to lose their jobs, hinder their access to health insurance, or even have their identity stolen.[31] Fertility data is a part of this especially sensitive class of data and has some privacy concerns of its own. The stigmas around this data alone can be incredibly harmful. More than half of all women experiencing infertility suffer from mental health issues from the stigma of infertility which can lead them to delay seeking out treatment.[32] In the same vein, stigmas around the use of contraceptives create challenges for women trying to access safe sexual and reproductive health.[33]

Beyond the psychological impact of this type of data being accessible, there are also more direct measurable harms that can be created when it is shared with third parties like employers, health care providers, or law enforcement. Employers could potentially use fertility data to identify who is using contraceptives, who is trying to get pregnant, or even who has lost or terminated pregnancies.[34] It is not hard to imagine how this data could directly or indirectly be used by employers to make important business decisions that could have major impacts on the women whose data was shared. Insurance companies can also change the availability or cost of their services for women depending on the type of health data they receive. Since pregnancy can be one of "the biggest and most unpredictable health-care expenses[,]" there is an almost certainty that insurance companies would do just that if given the chance.[35] With the recent

[28] Brooke Auxier et al., *4. Americans' Attitudes and Experiences with Privacy Policies and Laws*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.
[29] Jennifer Falk, *Federal Laws Needed to Protect Users from Confusing Privacy Policies, Research Shows*, THE DEN (Mar. 7, 2023), https://den.mercer.edu/federal-laws-needed-to-protect-users-from-confusing-privacy-policies-research-shows/.
[30] *See* NAT'L INST. OF HEALTH, *supra* note 22, at 93.
[31] *Id.*
[32] Yue Xie et al., *The Impact of Stigma on Mental Health and Quality of Life of Infertile Women: A Systematic Review*, FRONTIERS PSYCH., Jan. 9, 2023, at 1, 1–2.
[33] Annik Sorhaindo & Ulrika Rehnstrom Loi, *Interventions to Reduce Stigma Related to Contraception and Abortion: A Scoping Review*, BMJ OPEN, NOV. 2022, at 1, 1.
[34] *See* Rachel Wells, *Your Pregnancy App May Be Selling Your Data-to Your Boss*, GLAMOUR (Apr. 12, 2019), https://www.glamour.com/story/your-pregnancy-app-may-be-selling-your-datato-your-boss.
[35] Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?*, WASH. POST (Apr. 10, 2019, 3:11 PM), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.

overturning of *Roe v. Wade*, fertility data could even potentially be used as evidence in abortion prosecutions if shared with law enforcement.[36]

IV. Current Federal Regulations

As these fertility tracking apps and related technologies continue to grow in popularity and importance, the rules and regulations that govern them have been under increased scrutiny.

a. Federal Trade Commission (FTC)

The FTC was created in 1914 with the goal of "protect[ing] consumers and prompt[ing] competition."[37] This means that its role is to ensure that companies do not mislead consumers about how their data is being used.[38] However, this regulation is incredibly lacking when it comes to Femtech, as a question of law exists as to whether the information collected by these companies falls under the definition of protected health information (PHI).[39] At this time, the PHI definition only includes data collected by entities covered by HIPAA which, as will be discussed below, includes very few Femtech apps.[40] This means that the FTC only requires Femtech apps to have the same protection as any other mobile application without the increased protection of HIPAA.

With this limited role, the FTC only mandates that Femtech companies, just like any other company, must inform users of their policies; but does not regulate what those protection policies must be.[41] While the FTC has recognized that this gap in protection is of "growing concern," very little has been done to expand this regulation.[42] The Health Breach Notification Rule was expanded by the FTC to include health technologies but again, this only helps *after* a breach and does nothing to protect users from their data being taken in the first place.[43]

---

[36] Vittoria Elliott, *Fertility and Period Apps Can Be Weaponized in a Post*-Roe *World*, WIRED (June 7, 2022, 7:00 AM), https://www.wired.com/story/fertility-data-weaponized/.
[37] *Our History*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/history (last visited Aug. 15, 2024).
[38] *Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach (last visited Aug. 15, 2024).
[39] Celia Rosas, Note, *The Future is Femtech: Privacy and Data Security Issues Surrounding Femtech Applications*, 15 HASTINGS BUS. L. J. 319, 323 (2019).
[40] *See Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule*, *supra* note 38.
[41] Rosas, *supra* note 39, at 323–25.
[42] Kiana Baharloo, *Consumer News: Fertility Tracking Apps, DNA Testing, and…Vending Machines? Developments in FTC and State Protections on Certain Health Information*, 34 LOY. CONSUMER L. REV. 140, 140–41 (2022).
[43] *Id.* at 142.

b. Food and Drug Administration (FDA)

The FDA was created in 1906 to protect consumers of food and drugs from mislabeling and other misleading practices.[44] This role has expanded over the years and now the FDA is "responsible for advancing public health by helping to speed innovations that make medical products more effective, safer, and more affordable and by helping the public get the accurate, science-based information they need to use medical products . . . to maintain and improve their health."[45] To accomplish this goal, the FDA assigns new medical devices to one of three regulatory classes, where Class I is assigned the lowest-risk devices with the least regulation and Class III is assigned the highest-risk devices with the most stringent regulation.[46] Apps that dispense fertility and pregnancy information are classified as low-risk and thus require no agency approval before being placed on the market.[47] While other contraceptives like intrauterine devices (IUDs) and multiple-use female condoms (MUFCs) are designated as Class III devices, these "informational" apps maintain their low-risk status despite being marketed and used as contraceptives.[48]

One app has started to change this trend: Natural Cycles.[49] Natural Cycles was approved by the FDA and designated as a Class II device, requiring higher levels of protection.[50] While raising this standard is absolutely a step in the right direction, this could also be a potential hindrance to providing users of other Femtech apps with protection. This approval created a whole new category of medical devices for Software Applications for Contraception.[51] With Natural Cycles approval, other devices can now receive approval through FDA 510(k) submissions which simply require the device to be "at least as safe and effective" as existing, approved devices.[52] This means that any FTAs that can demonstrate its efficacy to be "substantially equivalent" to Natural Cycles can avoid the more rigorous approval process.[53] While this could speed up the approval process, some are rightfully concerned that the testing will become insufficient, resulting in less safe and effective products being released on the market.[54]

---

[44] *FDA History*, U.S. FOOD & DRUG ADMIN. (Jun. 29, 2018), https://www.fda.gov/about-fda/fda-history.
[45] *What We Do*, U.S. FOOD & DRUG ADMIN. (Nov. 21, 2023), https://www.fda.gov/about-fda/what-we-do.
[46] *Classify Your Medical Device*, U.S. FOOD & DRUG ADMIN. (Feb. 7, 2020), https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device.
[47] Taylor, *supra* note 9, at 2271.
[48] *Id.* at 2278–79.
[49] *Id.* at 2270.
[50] *Id.*
[51] *Id.* at 2271.
[52] *Id.* at 2280.
[53] *Id.*
[54] *Id.* at 2290.

c. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA was enacted in 1996 with the express goal of creating "national standards to protect sensitive patient health information . . . ."[55] The two main ways that HIPAA protects sensitive information is through its Privacy Rule and Security Rule. The Privacy Rule governs the use and disclosure of PHI and creates standards for individuals' rights to have control over their own PHI.[56] The Security Rule goes a step further and sets standards for how a certain subset of PHI in electronic form must be protected.[57] Unfortunately, these rules mostly do not apply to FTAs. "Covered entities" are those that have to follow these rules and only four specific groups fall into this classification: (1) health care providers; (2) health plans; (3) health care clearinghouses, or entities that standardize information from another covered entity; and (4) business associates, or organizations that use PHI to provide some service to another covered entity.[58] At this time, very few Femtech companies are considered to be covered entities and thus do not have to follow these rules that were created to protect personal health information.[59] One way data from FTAs or devices would be covered by HIPAA is if the user gets access to the technology as a benefit of their health care plan.[60]

d. Proposed Legislation

In response to the *Dobbs* decision taking away the federal right to abortion access, some members of Congress have introduced new legislation to combat hindered access.

i. My Body, My Data Act

Members of the House of Representatives introduced the *My Body, My Data Act* which proposes new standards that purportedly would protect personal reproductive health data across the nation.[61] The bill was first introduced in 2022 during the 117th Congressional Session and, after being reintroduced in the 118th Congressional Session, it was referred to the House Committee on Energy and Commerce which is where it is as of April 2024.[62] In perhaps the most bizarre way of accomplishing the purported goal or protecting personal reproductive health data, the Act would prevent this sensitive information from even being collected.[63] While preventing the creation of this data is of course one way of ensuring the data is not misused, this takes away all the benefits associated with FTAs and does not address the underlying issue of unsecured fertility

---

[55] *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CTR. FOR DISEASE CONTROL & PREVENTION (July 10, 2024), https://www.cdc.gov/phlp/publications/topic/hipaa.html.
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] Rosas, *supra* note 39.
[60] Erin Jones, *No, Health Data from Most Period-Tracking Apps Is Not Protected Under HIPAA*, VERIFY, https://www.verifythis.com/article/news/verify/health-verify/period-tracking-apps-hipaa-privacy-rules-law-fact-check/536-bf44e08c-cc5f-4ee8-997a-c15e0060081a (June 24, 2022, 2:26 PM).
[61] My Body, My Data Act of 2022, H.R. 8111, 117th Cong. (2022).
[62] *Id.*
[63] *Id.*

data. Aside from this odd minimization of data collection, the bill also has some promising proposals including a user's right of access, correction, and deletion, a privacy policy that regulated entities must abide by, and enforcement by the FTC.[64] The bill is supported by many pro-choice organizations including Planned Parenthood, Physicians for Reproductive Health, and the National Abortion Federation.[65]

ii. Protecting Personal Health Data Act

The Protecting Personal Health Data Act was introduced to the Senate in the 117th Congressional Session by Senator Amy Klobuchar with the express goal of "protect[ing] the personal health data of all Americans."[66] The bill was read to the Senate and referred to the Committee on Health, Education, Labor, and Pensions, where it still remains as of April 2024.[67] The Act recognizes that HIPAA does not provide the protection that is necessary in today's world with so many wearable fitness devices and health software on the market.[68] The bill introduces regulations for these devices and software that are not covered by HIPAA and that collect personal health data.[69] The bill proposes that the Department of Health and Human Services should enforce these regulations which makes sense given that the Department oversees HIPAA and the proposed regulations are very similar to those in HIPAA.[70] This Act could have the same effects as an expansion of HIPAA without having to amend that legislation.

V. Current State Protections

Since federal laws are lacking in terms of protection for users of Femtech and abortion access rights are now left to the states,[71] state legislators have had to step in to provide protection. A few examples of this happening include states passing their own consumer privacy laws,[72] and others adopting biometric privacy laws,[73] which could potentially be applied to FTAs.

a. Consumer Privacy Laws

California passed the California Consumer Privacy Act (CCPA) in 2018 with the express goal of securing more privacy for California consumers including several rights: (1) the right to know how their data is being collected, used, and shared; (2) the right to

[64] *Id.*
[65] *Sens. Wyden, Hirono, Rep. Jacobs Reintroduce the My Body, My Data Act to Protect Reproductive and Sexual Health Data*, RON WYDEN: U.S. SENATOR FOR OR. (May 18, 2023), https://www.wyden.senate.gov/news/press-releases/sens-wyden-hirono-rep-jacobs-reintroduce-the-my-body-my-data-act-to-protect-reproductive-and-sexual-health-data.
[66] Protecting Personal Health Data Act, S. 24, 117th Cong. (2021).
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *See generally* Dobbs v. Jackson Women's Health Org., 597 U.S. 215 (2022).
[72] Baharloo, *supra* note 42, at 144.
[73] *Is Biometric Information Protected by Privacy Laws?*, BLOOMBERG L. (June 20, 2024), https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/.

delete personal information upon request; (3) the right to opt-out of their personal data being sold or shared; and (4) the right to exercise these rights without discrimination.[74] The CCPA was then amended in 2020 to include the right to correct information that is inaccurate and the right to limit how sensitive information is used and disclosed.[75] As a state law, it only provides these rights to California residents.[76] It also only applies to businesses that either have annual revenues of more than $25 million, buy, sell, or share personal information of 100,000 or more Californians, or get 50% or more of their revenue from selling Californians' personal information.[77] This means that small businesses and non-profit organizations are not typically covered while government agencies are not covered by the law at all.[78] The conditions that must be met to actually bring an action against one of these businesses are also very limiting. A suit can only be successful if a user's non-encrypted and non-redacted personal information was taken in a data breach resulting from the business's failure to maintain "reasonable" security measures.[79] The damages are also capped at $750 per incident.[80] The CCPA even includes language requiring that a consumer provide a business that allegedly violates the act with notice, allowing them 30 days to cure the violation, which invalidates the suit.[81] Although this law only protects residents of California, this makes up over ten percent of the country's population,[82] and FTAs are definitely paying attention. Flo, Natural Cycles, Oura, and Glow all mention the CCPA in their privacy policies.

California passing this act seems to have started a trend. Fourteen other states passed state-specific consumer privacy laws since 2021 with many so new that they have not yet gone into effect.[83] Most of these statutes have very similar protections to those of California's law.[84] Virginia was the first state to follow in California's footsteps with the Virginia Consumer Data Protection Act which provides many of the same rights with the addition of requiring companies to assess their data protection standards.[85] As for Florida's law, there is some debate about its comprehensiveness since it only regulates companies that have over $1 billion in annual revenues and get more than half of that revenue from online ads.[86] Iowa's consumer privacy law is one of the more business-friendly acts as it does not give users the right to delete or collect data.[87]

---

[74] *California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa (Mar. 13, 2024).
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *In Brief*: *Your Rights Under the California Consumer Privacy Act*, CONSUMER ACTION (Dec. 29, 2022), https://consumer-action.org/english/articles/Brief-CCPA-Privacy-Rights.
[79] *California Consumer Privacy Act (CCPA)*, *supra* note 74.
[80] *Id.*
[81] *Id.*
[82] Bruce E. Cain & Preeti Hehmeyer, *California's Population Drain*, STAN. INST. FOR ECON. POL'Y RSCH. (SIEPR) (Oct. 2023), https://siepr.stanford.edu/publications/policy-brief/californias-population-drain.
[83] *Is Biometric Information Protected by Privacy Laws?*, *supra* note 73.
[84] *Which States Have Consumer Data Privacy Laws?*, BLOOMBERG L. (Mar. 18, 2024), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/.
[85] *Id.*
[86] *Id.*
[87] *Id.*

Oregon has some of the strongest data privacy with their Consumer Privacy Act passed in 2023 as it does not have many of the exemptions that other states include.[88] An additional eleven states have introduced, but not yet passed, their own consumer privacy bills.[89]

b. Biometric Data Protection

Generally speaking, Illinois is a leader in protecting biometric data. With the passage of the Biometric Information Privacy Act (BIPA) in 2008, Illinois became the first state to pass any biometric data privacy law.[90] Texas and Washington followed suit and passed broad biometric privacy laws.[91] Illinois was not just the first state to enact a law to protect biometric data but is also the most consumer-friendly.[92] Washington's consent requirement is the most lax of the three as it is "context-dependent" while the BIPA's is the strictest requiring that notice must state that bioinformation is being collected, the exact purpose for the collection, and length of time the data will be stored.[93] Washington and Texas, unlike Illinois, also allow biometric identifiers to be sold under specific circumstances outlined in the statute.[94] The BIPA is also unique in that no actual injury must be shown.[95] Instead, the statute creates a private right of action requiring just a technical violation,[96] which has been confirmed by the Illinois Supreme Court.[97] The Illinois State Supreme Court even further confirmed that each violation accrues damages even when the same biometric identifier of the same user is being collected or sold.[98] While these laws do nothing to protect data uploaded to apps by consumers themselves, it does help to secure personal data measured by biometric devices, like Apple watches and the Oura Ring.

VI. Privacy Terms

Under current regulations, Femtech mobile apps are free to use any security measures the company chooses despite the fact that these apps regularly have the same personal information as a physician or gynecologist.[99] Since most of the data stored in the apps is freely inputted by users, the data can be shared in ways that typical health data would never be shared. Several apps were found to share data with third parties like Facebook

[88] *Id.*
[89] *Id.*
[90] *Is Biometric Information Protected by Privacy Laws?*, *supra* note 73.
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] Baharloo, *supra* note 42, at 152.
[96] *See Is Biometric Information Protected by Privacy Laws?*, *supra* note 73.
[97] Baharloo, *supra* note 42, at 152.
[98] Kirk J. Nahra & Ali A. Jessani, *Illinois Supreme Court Finds that Biometric Information Privacy Act Claims Accrue with Each and Every Violation*, WILMERHALE (Feb. 23, 2023), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20230223-illinois-supreme-court-finds-that-biometric-information-privacy-act-claims-accrue-with-each-and-every-violation.
[99] Rosas, *supra* note 39, at 328–29.

and Google.[100] A UK-based study found that a majority of FTAs automatically transferred this data to Facebook as soon as the app was opened.[101] There has even been at least one case of a domestic violence victim being terrorized by her abuser with data he was able to get from the victim's fertility tracking app.[102] Perhaps most concerning on a large scale is the uncertainty around apps sharing this data with law enforcement through the third-party doctrine.[103]

This Note takes a closer look at the security, privacy, and effectiveness of four Femtech products on the market today: (1) Flo Period and Ovulation Tracker, which is the most downloaded female health app worldwide;[104] (2) Natural Cycles, which was approved by the FDA as a Class II device,[105] and was integrated with the wearable Oura Ring device; (3) Glow, which had a HIPAA compliant notice on its website;[106] and (4) Apple Health, the health app built into all iPhones.

a. Flo Period and Ovulation Tracker

In September 2023, the Flo Period and Pregnancy Tracker app (Flo) was the most popular female health app worldwide both by number of downloads and by revenue.[107] Unfortunately, this does not mean that it is the most accurate or the most secure. Although Flo's advertising suggests that it can be used as a form of birth control,[108] it is not approved for use as a contraceptive and most of the research done by the company relates to education and awareness.[109] However, this is not clear from the medical information tab on the website which describes, "[a]ccuracy you can count on" to make cycle predictions as precise as possible, implying that the app can be used as a form of birth control.[110]

In January 2021, the FTC brought a complaint against Flo alleging that it shared users' sensitive data as "app events" with marketing firms like Facebook and Google.[111] This

[100] Baharloo, *supra* note 42, at 146.
[101] Taylor, *supra* note 9, at 2272.
[102] *See* United States v. Madrigal, No. 3:22-cr-00019, 2023 WL 2823504, at *1, *12 (W.D.Va. Apr. 7, 2023).
[103] Elliott, *supra* note 36.
[104] Laura Ceci, *Leading Period Tracker and Female Health Apps Worldwide in September 2023, by Downloads*, STATISTA (Mar. 4, 2024), https://www.statista.com/statistics/1307702/top-period-tracker-apps-worldwide-by-downloads/.
[105] Taylor, *supra* note 9, at 2278–79.
[106] Rosas, *supra* note 39, at 322.
[107] Ceci, *supra* note 104; Laura Ceci, *Leading Period Tracker and Female Health Apps Worldwide in September 2023, by Revenues*, STATISTA (Mar. 4, 2024), https://www.statista.com/statistics/1307733/top-period-tracker-apps-worldwide-by-revenues/.
[108] Taylor, *supra* note 9, at 2283.
[109] *Science and Research at Flo*, FLO, https://flo.health/science-and-research (last visited Aug. 15, 2024).
[110] *Medical Accuracy and Expertise: Why You Can Trust Flo*, FLO, https://flo.health/medical-expertise (last visited Aug. 15, 2024).
[111] *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, FED. TRADE COMM'N (June 22, 2021), 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.

complaint was ultimately settled in a way that did not require Flo to admit to any wrongdoing and simply required Flo to receive consent before sharing users' health data in the future.[112] One of Flo's self-proclaimed guiding principles is to never sell personal data, and its website even claims that "[a]t no time has Flo ever sold user information to third parties for advertising purposes."[113] However, their own privacy policy provides a different picture. The policy explains that some "non-health" personal data is shared with AppsFlyer which then sends users' data out to "some of its integrated partners" which include Pinterest, Google, and Facebook.[114] No definition of what data is considered to be "non-health" is provided. The privacy policy also freely admits that data may be de-identified and shared with third parties.[115] So, although Flo claims to not share data with third party advertisers, its own policy expresses that users' data will be shared with a company that will do just that.

Beyond the data that is user-generated within the app, Flo automatically collects other personal data including data from third parties, device information, and even location information.[116] The policy also goes on to explain that data may be shared "[i]n response to subpoenas, court orders, or legal processes, to the extent permitted and as required by applicable law . . . ."[117] It is important to note the wording here that explains that data will not just be shared when required but also "to the extent permitted . . . ."[118] Under the third-party doctrine as it stands now, this is an incredibly low threshold.

Flo does recognize the dread that some people might feel sharing this much of their personal data so it does offer some ways for users to do more to protect their privacy including an anonymous mode and the ability for users to delete their data.[119] The anonymous mode allows users to create an account without any identifying information, but there are some limitations to what the app can do when your personal information is removed.[120] In anonymous mode, all data will be lost if a user's device is stolen or even if the user gets a new phone.[121] An anonymous user is also unable to pair the app with a wearable device or communicate with the Flo Support team.[122] For some reason, these are incredibly important features that Flo would prefer not to forgo.

If a user decides that using the app is no longer in her best interest, the user can deactivate her account and ask that all her personal information be deleted.[123] However,

[112] Sara Merken, *Women's Health App Maker Settles FTC Claims over Data Disclosure*, WESTLAW TODAY (Jan. 13, 2021, 11:16 PM), https://today.westlaw.com/Document/I39b9682055f611eb9ec1f9139cc451ff/View/FullText.html?transitionType=SearchItem&contextData=(sc.Default)&firstPage=true.
[113] *Your Body. Your Data.*, FLO, https://flo.health/privacy-portal (last visited Aug. 15, 2024).
[114] *Flo Privacy Policy*, FLO, https://flo.health/privacy-policy (last visited Aug. 15, 2024).
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Anonymous Mode FAQ*, FLO, https://flo.health/privacy-portal/anonymous-mode-faq (last visited Aug. 15, 2024).
[122] *Id.*
[123] *Your Body. Your Data.*, *supra* note 113.

this deletion can take up to 90 days to be completed and, if a user simply deletes the app and does not go through the deletion request process, her data will be stored for three years.[124] Flo's privacy policy also explains that some personal data may be kept even after this deletion process "as necessary to comply with legal obligations; establishment, exercise or defense of legal claims; and for archiving purposes in the public interest, scientific or historical research or statistical purposes."[125]

There are also some concerns about the security of the data collected by Flo. In order to give users the most accurate tracking information, Flo has to keep some personal data as long as a user is active.[126] Since Flo is not an FDA-approved device or controlled by HIPAA, there are no regulations as to how it must store this data, but Flo does provide its commitment to comply with the General Data Protection Regulation. While Flo itself reports to encrypt users' data and store it on "the most secure cloud computing environment available[,]"[127] it is apparent from the previously mentioned FTC complaint that Flo does not always follow through on its promises.[128] However, given this recent controversy, Flo is under a more critical eye and hopefully has shaped up its privacy measures to prevent any further complaints. Perhaps unsurprisingly, given the recent change in abortion law, Flo features an answer to the frequently asked question of risk related to abortion access and sharing data with Flo.[129] In response to the question of risk, Flo proclaims the following:

> Your health data will never be shared with any company but Flo. Beyond this, we will never require you to log an abortion or offer details that you feel should be kept private. Should you have any concerns about the data you've submitted, please reach out to our Customer Support team who will ensure all historical data has been deleted. We firmly believe that our users deserve complete control over their data and we are here to support you every step of the way.[130]

Although this statement sounds promising, it is not exactly consistent with what Flo says in their privacy policy and it is unclear if data will be shared at the request of law enforcement hoping to enforce an abortion prosecution.

---

[124] *Flo Privacy Policy, supra* note 114. (The statute of limitations in states that have banned abortions is almost always longer than this period).
[125] *Id.*
[126] *Id.*
[127] *Where Is My Data Stored?*, FLO, https://help.flo.health/hc/en-us/articles/360042626751-Where-is-my-data-stored (last visited Aug. 15, 2024).
[128] *Flo Ovulation & Period Tracker*, MOZ://A (Aug. 9, 2022), https://foundation.mozilla.org/en/privacynotincluded/flo-ovulation-period-tracker/.
[129] *If I'm Having an Abortion in the US, Am I at Risk Whilst Using Flo?*, FLO, https://help.flo.health/hc/en-us/articles/6498122107028-If-I-m-having-an-abortion-in-the-US-am-I-at-risk-whilst-using-Flo (Last visited Aug. 15, 2024).
[130] *Id.*

b. Natural Cycles and Oura Ring

Natural Cycles was the first (and, so far, the only) fertility app to be approved by the FDA.[131] It was cleared as a form of birth control under the Class II regulatory class in 2018.[132] The website claims that Natural Cycles is 93% effective with typical use which can increase to 98% effectiveness with perfect use.[133] This is further supported by a study conducted by the Swedish Medical Products Agency which found that the app had a failure rate of 6.9% with typical use.[134] When used in conjunction with Oura, a user gets closer to perfect use since the ring takes the user's temperature on a more regular and consistent basis than an individual will on her own.[135] The effectiveness ultimately stays the same though.[136]

Natural Cycles has special safety concerns to consider as it has a partnership with Oura Ring, a wearable device that measures body temperature to provide a more accurate fertility treatment.[137] With FDA approval and integration with a wearable device, there are of course higher standards for data security. The type of data that Natural Cycles collects is very similar to Flo. Once again, a lot of the data is user-inputted, but with the Oura Ring integration, the data is even more accurate and personal. Even without the Oura Ring, Natural Cycles automatically collects data including device information, marketing data, and even location data.[138]

Natural Cycles' privacy policy is more upfront than that of Flo, but once again, the data collected is shared for marketing purposes.[139] There is the option for users to opt out of this data sharing either in the settings or by contacting the app's support team, but the presumption is that the data will be shared.[140] The privacy policy also explains that the app will share data for scientific research although consent is required for this and all the data is pseudonymized or anonymized.[141] Beyond that, the policy outlines several other recipients of personal data including service providers, affiliates, and those who users ask Natural Cycles to share data with.[142] The policy also outlines that it will respond to legal third-party inquiries "only if required" and further explains that it "will contest the disclosure of your personal data in response to a third-party inquiry to the

[131] Taylor, *supra* note 9, at 2290.
[132] *Id.*
[133] *Prevent Pregnancy with Natural Cycles*, NAT. CYCLES, https://www.naturalcycles.com/is-natural-cycles-right-for-me (last visited Aug. 15, 2024).
[134] Taylor, *supra* note 9, at 2276.
[135] *How Does the Oura Ring Work with Natural Cycles?*, NAT. CYCLES, https://help.naturalcycles.com/hc/en-us/articles/6050918780445-How-does-the-Oura-Ring-work-with-Natural-Cycles (last visited Aug. 15, 2024).
[136] *Id.*
[137] *Oura Integrates with FDA-Cleared Birth Control App, Natural Cycles*, OURA, https://ouraring.com/blog/oura-partners-with-fda-cleared-birth-control-app-natural-cycles/ (last visited Aug. 15, 2024).
[138] *Privacy Policy*, NAT. CYCLES, https://www.naturalcycles.com/other/legal/privacy (Dec. 4, 2023).
[139] *Id.*
[140] *Id.*
[141] *Id.*
[142] *Id.*

extent that a reasonable ground for objection exists."[143] The policy even explains that they will provide users with notice that a request has been made as legally permitted.[144]

Just like Flo, Natural Cycles saves users' data for three years after users stop using their accounts.[145] The privacy policy states that a user's data will be anonymized if consent is withdrawn or if the user's erasure request is successful.[146] The policy is clear that the data will be anonymized and will not be used in any of Natural Cycles' research but makes no mention of actual deletion.[147]

As a Swedish company with FDA approval, personal data provided to Natural Cycles is protected under the General Data Protection Regulation and complies with the FDA's cybersecurity requirements.[148] It also describes its own privacy requirement, *NC° Secure*, on top of those regulations.[149] The policy says that all information provided to the app is encrypted and stored on secure servers, generally accepted industry standards are used, and "strict procedures" are in place for any possible data breaches.[150]

Although Natural Cycles is advertised and approved as a form of contraceptive, there is very little mention of abortion on the website. There is an article describing how to log an abortion in the app,[151] but unlike Flo, Natural Cycles only makes vague mentions of the recent overturning of the federal right to abortion access.

Oura has its own privacy policy that is also adhered to when the app and the ring are used together. Very similar data is collected including contact information and location data but with the addition of measured and calculated data such as heart rate, temperature data, sleep phases, and BMI.[152] Oura also processes marketing data but claims not to sell data to any third parties.[153] Oura has one of the strongest stances against sharing data with law enforcement, stating that they "will oppose any request to provide legal authorities with . . . data for surveillance or prosecution purposes[,]" and expresses that any user whose data is requested will receive a notification.[154]

The data collected by Oura is typically retained as long as the user's account remains active.[155] Its policy does however provide that data will be deleted when the purpose it

[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] *Welcome to NC Secure*, NAT. CYCLES, https://www.naturalcycles.com/secure (last visited Aug. 15, 2024).
[149] *How to Delete Your Natural Cycles Account*, NAT. CYCLES, https://help.naturalcycles.com/hc/en-us/articles/360006694278-How-to-delete-your-Natural-Cycles-account (last visited Aug. 15, 2024).
[150] *Privacy Policy*, *supra* note 138.
[151] *How to Use the App After an Abortion*, NAT. CYCLES, https://help.naturalcycles.com/hc/en-us/articles/360011012637-How-to-use-the-app-after-an-abortion (last visited Aug. 15, 2024).
[152] *Oura Health Privacy Policy*, OURA, https://ouraring.com/privacy-policy-oura-health (May 2, 2024).
[153] *Id.*
[154] *Id.*
[155] *Id.*

was originally collected for has been completed unless there is some legal obligation to keep it for longer.[156] Just like with Flo, a user may request for her account to be deleted and this request will be complied with unless Oura has a legal basis not to or is legally required to preserve the data.[157] Oura also describes the right that users have to withdraw their consent to having their data processed at any time although this could affect the usability of the product.[158]

The Oura Ring has received the same FDA clearance as Natural Cycles through an FDA 510(k) clearance so all of the same data protection requirements apply.[159] Oura uses a similar process of anonymization or pseudonymization of personal data, restricting access, and using encryption when possible.[160]

One twist that comes with Oura Rings is the availability of "Oura for Business" which allows companies to provide employees with Oura Rings as a part of their wellness missions.[161] When medical devices are integrated into employer health plans, there is an increased risk of personal data being misused as employers can then access the data collected from their employees.[162] Oura is no different, providing "recommendations" to business leaders based on data collected from individual employees.[163] Since this data is anonymized and aggregated,[164] it can be used for positive change in a company's wellness plan.[165] However, it is easy to see how this information could be misused by companies, even to identify and retaliate against women based on information they provide the app in confidence.[166]

c. Glow Fertility and Ovulation App

After an analysis of the privacy policies of several FTAs, Glow appears to be the only one to have ever provided a HIPAA compliance statement.[167] In an old version of Glow's privacy policy from 2018, it claims to store data with "HIPAA compliant policies,"[168] but it is unclear what this means since Glow is not a HIPAA covered

---

[156] *Id.*
[157] *Id.*
[158] *Id.*
[159] *Natural Cycles Receives FDA Clearance to Integrate Its Birth Control App with Data Measured by Apple Watch*, PR NEWSWIRE (Sep. 19, 2023, 8:25 AM), https://www.prnewswire.com/news-releases/natural-cycles-receives-fda-clearance-to-integrate-its-birth-control-app-with-data-measured-by-apple-watch-301931262.html.
[160] *Oura Health Privacy Policy*, *supra* note 152.
[161] *Oura for Business*, OURA, https://ouraring.com/business (last visited Aug. 15, 2024).
[162] Taylor, *supra* note 9, at 2294.
[163] Jessica Hagen, *Wearable Company Oura Launches Employer Program*, MOBIHEALTHNEWS (Dec. 1, 2022, 1:00 PM), https://www.mobihealthnews.com/news/wearable-company-oura-launches-employer-program.
[164] Annie Burky, *Oura Launches Employer-Focused Wellness Arm*, FIERCE HEALTHCARE (Dec. 2, 2022, 3:15 PM), https://www.fiercehealthcare.com/digital-health/oura-business-has-already-worked-200-orgs-throughout-commerce-provide-insight.
[165] Taylor, *supra* note 9, at 2294.
[166] *Id.* at 2294–95.
[167] Rosas, *supra* note 39, at 322.
[168] *Glow Privacy Policy*, GLOW, https://perma.cc/82FN-A98R (May 25, 2018).

entity.[169] This is essentially a meaningless phrase which is probably why the HIPAA compliance notice was last included in the privacy policy in the 2020 update.[170]

This change was likely due at least in part to the California Attorney General's settlement with Glow after an investigation into alleged privacy and security failures.[171] The most worrisome part of the complaint brought against the app alleged that the password change function had security issues that may have allowed third parties to reset a user's password and access the user's account without the user's consent or knowledge.[172] This is of course incredibly alarming that third parties may have been able to readily access a user's information of a very personal nature. As with the Flo-FTC settlement, no wrongdoing was ever admitted but the settlement included a $250,000 civil penalty, some injunctive terms about compliance with state privacy laws, and, in a new form of injunction, a requirement that Glow considers how lapses in its security "may uniquely impact women."[173]

The Glow privacy policy of today of course looks quite a bit different than it did before that settlement. In addition to the data provided by users, the app also automatically collects much of the same data as Flo and Natural Cycles including device data, online activity data, and location data.[174] Glow also has a sort of social media aspect in which a user's profile is shared with the public by default and a user who wishes not to have her profile be public must opt out of this option.[175] Users can opt into having their data shared with other mobile health applications, but users presumptively provide consent to having their data shared with third-party advertisers with an option to opt out.[176] The policy goes on to explain that Glow will share user data with law enforcement "as [it] believe[s] in good faith to be necessary or appropriate for the compliance and protection purposes . . . ."[177] This is by far the least stringent policy about sharing data with law enforcement out of the three apps explored in this Note.

Similarly to Natural Cycles, Glow provides the option for users to either delete their data or revoke consent at any time.[178] The policy provides that a deletion request will be processed and completed within 30 days.[179] The revocation of consent only applies to

[169] Jones, *supra* note 60.
[170] *Glow Privacy Policy*, GLOW, https://glowing.com/privacy-20200331 (Mar. 31, 2020).
[171] *Attorney General Becerra Announces Landmark Settlement Against Glow, Inc. – Fertility App Risked Exposing Millions of Women's Personal and Medical Information*, U.S. DEP' T OF HEALTH AND HUM. SERVS. (Sep. 17, 2020), https://oig.hhs.gov/fraud/enforcement/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-fertility-app-risked-exposing-millions-of-womens-personal-and-medical-information/.
[172] *Attorney General Becerra Announces Landmark Settlement Against Glow, Inc. – Fertility App Risked Exposing Millions of Women's Personal and Medical Information*, STATE OF CAL. DEP'T OF JUST. (Sep. 17, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93.
[173] *Id.*
[174] *Glow Privacy Policy*, GLOW, https://glowing.com/privacy-policy (May 21, 2024).
[175] *Id.*
[176] *Id.*
[177] *Id.*
[178] *Id.*
[179] *Id.*

certain data and, if a user wants to revoke consent beyond what is permissible in the "your choices" section of the privacy policy, the user must delete her account.[180] Interestingly, Glow provides a third option that allows users to delete their "Key Health Data" from the servers and just store it on their personal devices.[181] Since this means that the data will only be shared locally, there will of course be some app features that no longer function.[182]

The security portion of Glow's privacy policy is concerningly lacking. It claims that "a number of technical, organizational and physical safeguards" are used but does not describe what these safeguards are.[183] It even goes on to say that "security risk is inherent" and the security of a user's personal data cannot be guaranteed.[184] This is a huge contrast to the previous versions of Glow's privacy policy that claimed its security was HIPAA compliant although, as previously discussed, these two statements are not functionally all that different.

d. Apple Health

Apple Health is the mobile health app that is provided on all iPhones. It has basic cycle tracking abilities built into it which provides more data protection than typical apps sold in the app store.[185] Like Natural Cycles, it can also be easily integrated with wearable devices, especially the Apple Watch.[186] When iPhone users have some form of lock on their phones, like a passcode, Touch ID, or Face ID, the data in the Apple Health app is encrypted and Apple does not keep or have access to the encryption key.[187] With a device updated to at least iOS 12 and two-factor authentication, Apple is unable to access the data even if it is synced with the user's iCloud.[188] The data collected by the app can be shared with other third parties, friends and family, or health care providers as the user chooses, but this of course makes the information inherently less secure as more entities have access to it.[189] Apple further reiterates that these protections also apply to data provided for cycle tracking.[190] The privacy policy for the Apple Health app also provides information about how the data is retained and how to go about removing the data as a user may choose. Apple explains that the health data is stored in the app

[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] *Id.*
[185] Tatum Hunter & Heather Kelly, *With Roe Overturned, Period-Tracking Apps Raise New Worries*, WASH. POST (June 24, 2022, 2:30 PM), https://www.washingtonpost.com/technology/2022/05/07/period-tracking-privacy/.
[186] *See Health App & Privacy*, APPLE LEGAL, https://www.apple.com/legal/privacy/data/en/health-app/ (last visited Aug. 15, 2024).
[187] *Id.*
[188] *Id.*
[189] *Id.*
[190] *Log Menstrual Cycle Information in Health on iPhone*, IPHONE USER GUIDE, https://support.apple.com/guide/iphone/log-menstrual-cycle-information-iph51a822b18/ios (last visited Aug. 15, 2024).

and, if a user chooses, in iCloud.[191] Users can also review, edit, or delete their data at any time.[192]

As for sharing data with law enforcement, Apple has a clear stance that it will only share data with law enforcement when law enforcement has a valid legal basis that is not "unclear, inappropriate, or overly broad . . . ."[193] Apple even publishes a report every six months outlining how many requests it received, what was requested, and how often data was provided.[194] While Apple outlines a strict stance of sharing data only as necessary and rejection of most private party requests, around 90% of all requests from the government were complied with.[195] Apple has been very careful about curating a reputation of being a front runner in data privacy, but the rates at which it shares data with law enforcement does not support this position.[196]

VII. Drawbacks of Femtech

a. Dependability

While many fertility apps are marketed as digital extensions of contraception,[197] the efficacy of these apps for that use is highly suspect. While the ability to track one's own cycle can provide a woman with a greater sense of autonomy, the dependence on user input also makes the contraceptive ability of the apps less effective.[198] Since all FTAs, except Natural Cycles, have no duty to provide data about their effectiveness, it is unclear what their efficacy rates are. Some experts explain that, despite these apps directly advertising or simply implying their ability to be used as contraceptives, they are not much more advanced than the old-fashioned rhythm method using a calendar-based approach.[199] Despite this lack of efficacy data, almost 75% of women using fertility apps for contraception purposes were either very confident or somewhat confident that the app would help them avoid becoming pregnant.[200] If the federal government will not ensure the right to abortion access, the least it could do is regulate FTAs to ensure efficacy and negate the necessity of abortion procedures.

---

[191] *Health App & Privacy*, *supra* note 186.
[192] *Id.*
[193] *We Believe Security Shouldn't Come at the Expense of Individual Privacy.*, APPLE PRIVACY, https://www.apple.com/privacy/government-information-requests/ (last visited Aug. 15, 2024).
[194] *See United States of America Transparency Report*, APPLE PRIVACY, https://www.apple.com/legal/transparency/us.html (last visited Aug. 15, 2024).
[195] *Id.*
[196] Johana Bhuiyan, *Apple Says It Prioritizes Privacy. Experts Say Gaps Remain*, THE GUARDIAN (Sep. 23, 2022, 11:00 AM), https://www.theguardian.com/technology/2022/sep/23/apple-user-data-law-enforcement-falling-short.
[197] Mary Summer Starling et al., *User Profile and Preferences in Fertility Apps for Preventing Pregnancy: An Exploratory Pilot Study*, MHEALTH, June 2018, at 1, 2.
[198] Taylor, *supra* note 9, at 2289.
[199] *Id.* at 2276.
[200] *Id.* at 2275.

b. Sharing Data with Law Enforcement

The Fourth Amendment protects the right to be secure from unreasonable searches and seizures.[201] However, this only provides protection from the government infringing on these rights, not third parties.[202] This means that law enforcement is able to obtain information that is voluntarily turned over by third parties that have the authority to do so without it being considered an illegal search.[203] Since users voluntarily upload cycle data and consent to their location data being tracked, the doctrine means that no expectation of privacy from law enforcement interference exists for this data. These apps are then permitted to turn over data about a user's menstrual cycle and location upon a simple request from law enforcement. This is why the apps' stance on sharing data with law enforcement is so crucial.

Flo's policy of sharing data with law enforcement "to the extent permitted" and Glow's policy to share data with law enforcement when they believe it to be necessary or appropriate is thus concerning to users hoping to avoid prosecution if the users need to get an abortion procedure. In accordance with both of these apps' data collection and privacy terms, they could turn over a user's cycle data showing a missed period or location data showing a user at a women's health care facility, both of which could be used as evidence in an abortion prosecution. Natural Cycles and Oura provide a bit more hope of protection in their privacy policies promising to contest disclosures under third-party inquiries, provide users with notice of third-party requests as permitted, and only disclose data as required. Unfortunately, no matter how much an app may contest sharing its users' data by means of the third-party doctrine, they must comply with subpoenas for personal data.

c. Workers' Rights

As previously discussed, some Femtech devices are provided through employer health plans.[204] These company-wide subscriptions to FTAs provide users' data to internal employer websites.[205] Theoretically, this data can be used to assess employees' health and promote "corporate wellness," but it is not hard to imagine how this data could instead be used to identify and retaliate against pregnant women, women who have an abortion, women trying to get pregnant, or even just women using contraception.[206] FTAs collect data related to all these classifications. Although Title VII of the Civil Rights Act's prohibition against sex discrimination includes all of the aforementioned categories,[207] a claim of this nature requires showing that the employer was aware of the

[201] U.S. CONST. amend. IV.
[202] Smith v. Maryland, 442 U.S. 735, 745 (1979).
[203] *Id.*
[204] Taylor, *supra* note 9, at 2294.
[205] *Id.*
[206] *Id.* at 2295.
[207] *Pregnancy Discrimination and Pregnancy-Related Disability Discrimination*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/pregnancy-discrimination (last visited Aug. 15, 2024).

employee's status in one of these protected classes.[208] While the apps that share data with employers claim that the data is de-identified and aggregated, a company with a small number of women of reproductive age could easily identify which of their employees got an abortion, use birth control, or are pregnant or hoping to become pregnant and retaliate against them.

VIII. Goals and Solutions

The U.S. Department of Health and Human Services recognizes reproductive health care as an essential part of overall health and well-being.[209] It is increasingly apparent that many state legislators do not feel the same or, at the very least, think that other considerations are more important as so many states have enacted bans on abortion, a fundamental aspect of reproductive health. A study has shown that these bans not only restrict access to abortions but even make it harder for women to get general reproductive health care like routine check-ups and contraceptives.[210] In 2017, 40.6% of women reported experiencing at least one barrier to reproductive health care services which jumped up to 44.6% in 2021.[211] Providing access to personal health information and protecting that data is now more important than ever.

a. Increased Awareness

As discussed previously, many women who use fertility apps as a form of contraception were found to be at least somewhat confident in the app's ability to help them avoid pregnancy despite the efficacy being, with a generous estimate, around 93%.[212] FTAs also often present themselves as forms of contraception that keep data safe from third parties and law enforcement. Given these common misconceptions, increased awareness can be a huge step in the right direction. It can put pressure on Femtech companies to provide more security, encourage politicians to work to introduce legislation with more protections for consumers, and allow women to make more informed decisions about how they share their data and who they share it with.

There is even an entity already in place that can accomplish this goal of increasing awareness with the right support: the Office of Women's Health (OWH).[213] OWH was created by the FDA in 1994 with the mission of serving as an advisor to government agencies on issues related to women's health, promoting the inclusion of women in

---

[208] *Id.*
[209] *Know Your Rights, Reproductive Health Care*, U.S. DEP'T OF HEALTH AND HUM. SERVS. (June 25, 2022), https://www.hhs.gov/about/news/2022/06/25/know-your-rights-reproductive-health-care.html.
[210] Deidre McPhillips, *Access to Reproductive Health Care Has Become More Challenging for Women in the US, Study Shows*, CNN HEALTH (Apr. 10, 2023, 7:22 PM), https://www.cnn.com/2023/04/10/health/reproductive-health-barriers-wellness/index.html.
[211] Aliza Adler et al., *Changes in the Frequency and Type of Barriers to Reproductive Health Care Between 2017 and 2021*, JAMA NETWORK OPEN, Apr. 2023, at 1, 8.
[212] Taylor, *supra* note 9, at 2290.
[213] Genevieve Grabman & Cara Tenebaum, *FDA Regulation Must Uphold Women's Health*, 77 FOOD & DRUG L.J. 318, 318 (2022).

medical research, and identifying new challenges to women's health.[214] The Office has a program area specific to outreach that could take on this goal if the FDA provides it with adequate support.[215] However, awareness without meaningful change in data protection guidelines will force women to choose between taking advantage of new technologies specifically made for them and keeping their data secure which is not a fair decision.

b. Raise FDA Classification Level

A potential solution to address the issue of reliability of these FTAs is to raise their FDA classification from low-risk devices, that require no agency as they are now, to a Class II or even Class III regulatory class.[216] The FDA defines Software Applications for Contraception (SACs) as "a device that provides user-specific fertility information for preventing a pregnancy" which sounds an awful lot like what FTAs purport to do or lead customers to believe they do.[217] These SACs are Class II devices requiring FDA approval and several special controls.[218] Since FTAs perform the same function as these SACs, it seems they should be classified the same way. This raise of classification would require that FTAs show clinical efficacy, conduct performance evaluations to ensure users can use the app correctly based on the directions provided, implement higher safety requirements, and comply with FDA labeling requirements.[219] This would address the issue of dependability of the apps, increase security of the data they collect, and even raise awareness for the women who choose to use them, addressing all the goals outlined here.

The issue that comes with including FTAs in the Class II classification level is that the approval process is a bit hindered by the FDA 510(k) process. As previously discussed, the FDA provides a de novo pathway for Class I or II devices that can show they are "at least as safe and effective" as a previously approved device.[220] Since Natural Cycles is already approved and marketed as a Class II device, it can now serve as a predicate device for all FTAs hoping to be approved, meaning they would only have to show they are "substantially equivalent" to Natural Cycles.[221] This removes a huge barrier for FDA approval which could help speed up innovation, but it also means that the apps hoping to get approved don't have to go through a rigorous verification process.

While it seems unlikely since these apps do not even require FDA approval currently, this Note proposes that FTAs be raised past Class II and all the way up to Class III.

---

[214] *Office of Women's Health*, U.S. FOOD & DRUG ADMIN. (July 30, 2024), https://www.fda.gov/about-fda/office-commissioner/office-womens-health.
[215] *Id.*
[216] Taylor, *supra* note 9, at 2293.
[217] 21 C.F.R. § 884.5370 (2023).
[218] Taylor, *supra* note 9, at 2279.
[219] *Id.* at 2287–88.
[220] *Id.* at 2280.
[221] *Id.*

IUDs (hormonal and non-hormonal) are currently regulated at this level,[222] and although FTAs are certainly less physically invasive, the sensitive data collected by these apps should make them equivalent for regulation purposes. The FDA describes Class III devices as "ones that . . . [are] of substantial importance in preventing impairment of human health or present[] a potential, unreasonable risk of illness or injury."[223] This definition absolutely seems to encompass technology that claims to prevent pregnancy. While an unplanned pregnancy isn't exactly an illness or injury, it is not at all a stretch to say that it would be an impairment of human health. Any woman who becomes pregnant absolutely has her health impaired. The safest pregnancies come with back pain, headaches, indigestion, rapid weight gain, and nausea at essentially the bare minimum.[224] These alone are impairments of human health and this isn't even mentioning the more severe health problems that can be caused by or more likely to happen during pregnancy including anemia, gestational diabetes, bacterial infections, and preeclampsia.[225] If apps are advertised as able to prevent pregnancy and all of these complications that come along with it, they absolutely are of substantial importance in preventing the impairment of human health and should be regulated as such.

c. HIPAA Expansion

As it stands now, HIPAA is too narrowly tailored and does nothing to protect users of FTAs even though these apps are regularly provided with information that is just as sensitive as information provided to primary care physicians and gynecologists. An expansion of HIPAA to include these apps would create a requirement that they all follow HIPAA's Privacy Rule, Security Rule, and Breach Notification Rule which are currently meaningless to FTAs.[226] Application of the Privacy Rule would require these apps to use and disclose user data in compliance with HIPAA rather than leaving them up to their own discretion as they are now. Applying the Security Rule would mandate that FTAs comply with security regulations set forth by the Department of Health and Human Services instead of allowing FTAs to decide on their own unregulated safety measures. While data breaches of FTAs are currently only communicated to users when an FTC complaint is filed,[227] applying HIPAA's Breach Notification Rule would require the apps to make users aware when their information is leaked.

But how could this be done? For HIPAA to apply, an entity must be classified as either a health care provider that electronically transmits health information, a health plan, a health care clearinghouse, or a business associate of one of those entities.[228] Health

[222] *Id.* at 2288.
[223] *PMA Approvals*, U.S. FOOD & DRUG ADMIN. (May 29, 2024), https://www.fda.gov/medical-devices/device-approvals-and-clearances/pma-approvals.
[224] *Common Health Problems in Pregnancy*, NAT'L HEALTH SERVS. (Apr. 22, 2024), https://www.nhs.uk/pregnancy/related-conditions/common-symptoms/common-health-problems/.
[225] *Pregnancy Complications*, OFF. ON WOMEN'S HEALTH, https://www.womenshealth.gov/pregnancy/youre-pregnant-now-what/pregnancy-complications (Dec. 29, 2022).
[226] Rosas, *supra* note 39, at 331–32.
[227] Baharloo, *supra* note 42, at 145–46.
[228] 45 C.F.R. § 160.103.

plans are those plans that provide or pay for the cost of medical care.[229] Health care clearinghouses are entities that "process[] or facilitate[] the processing of health information received from another entity in nonstandard format . . . ."[230] Neither definition is a great fit for FTAs. However, this Note contends that a legitimate argument can be made that FTAs should be considered health care providers or, at the very least, the definition of business associates should be expanded to include them.

The statute defines health care providers as those who provide "medical or health services . . . ."[231] The statute goes on to provide an extensive list of what medical and health services are which includes physician services and personalized preventive plan services.[232] While there is no precedent for defining FTAs as health services, it seems clear that, if not physician services, they at least provide these personalized preventive plans. FTAs provide recommendations (estimated ovulation dates) based on health information (cycle data) of each individual. However, this Note recognizes that it is incredibly unlikely that any agency or court would find that FTAs are in fact health care providers; expanding the definition of business associates would likely be an easier way to provide HIPAA protections. FTAs absolutely provide the services of business associates,[233] but they do not do so on behalf of covered entities, so they are not regulated by HIPAA. A removal of this requirement would allow HIPAA to govern FTAs and provide users with the protection they need and deserve.

IX. Conclusion

As the use of fertility tracking apps and wearable devices continues to increase, it has become increasingly important to keep women's health data private to keep women protected from discrimination in the workplace, unfair prejudice in the insurance field, loss of personal autonomy and, with the recent *Dobbs* decision, even criminal prosecution. Current regulations such as those provided by the Federal Trade Commission, the Food and Drug Administration, and the Health Insurance Portability and Accountability Act are limited to the point of being almost inconsequential. Policy change is needed to provide better privacy and security for women's reproductive health data.

[229] *Id.*
[230] *Id.*
[231] *Id.*
[232] *Id.*; *see also* 42 U.S.C. § 1395x.
[233] Data transmission of health information, offer personal health records, and create, receive, maintain, or transmit protected health information. 45 C.F.R. § 160.103.