NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 23 | Issue 3 Article 6

4-1-2022

This is No Ovary-Action: Femtech Apps Need Stronger Regulations to Protect Data and Advance Public Health Goals

Allysan Scatterday

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 23, ISSUE 3: APRIL 2022

THIS IS NO OVARY-ACTION: FEMTECH APPS NEED STRONGER REGULATIONS TO PROTECT DATA AND ADVANCE PUBLIC HEALTH GOALS

Allysan Scatterday*

Millions of people download and use "femtech," or female technology, applications to track patterns in their reproductive health, including menstruation and fertility. The market for femtech apps is projected to experience rapid growth over the next decade. Despite the highly sensitive, intimate nature of data collected by femtech apps, U.S. privacy law leaves these apps largely unregulated. Recent investigations reveal that femtech app developers have misled users about their privacy policies, left user accounts vulnerable to security threats, and sold user data to advertisers and other third parties without notice or consent. Femtech app users urgently need legal solutions that strengthen privacy protections; however, along with maintaining data privacy, proposed actions should also address ways to use data collected by femtech apps to fill critical gaps in women's health research.

* J.D. Candidate, University of North Carolina School of Law, 2023. The Author would like to thank the NC JOLT staff members and editors, particularly Meg Daly, Meredith Doswell, and Anna Comer, for their guidance, support, and thoughtful feedback throughout the editorial process. The Author would also like to thank her family and friends—particularly her spouse, Alex—for the non-editorial support.

TABLE OF CONTENTS

I. INTRODUCTION

Consider this paradox: a thirty-year-old person, who has been trying to conceive their second child for three years, visits an obstetrician after recently experiencing a fourth miscarriage. They share details with the physician regarding their physical and mental health symptoms, their most recent menstrual cycle, and their sexual history. Because the doctor's office is a healthcare provider, all of the information the patient shares will remain confidential unless

they provide written authorization consenting to disclosure.[1] Although the obstetrician records data from the appointment electronically, the doctor's office is required to implement technological safeguards to ensure that the information remains secure.[2] After arriving home from the appointment, the patient opens a fertility-tracking app on their phone and records the same personal health information that they shared with their doctor. Unfortunately, current laws do not require the app to maintain the privacy or security of that data.[3] In fact, the app can profit off of the data, selling it to advertisers and third parties without providing notice or receiving consent.[4]

This hypothetical represents reality for millions of users of female technology, or "femtech,"[5] apps in the United States today. This Article explores the complex issues surrounding data collected by femtech apps and emphasizes the need to strengthen privacy protections while simultaneously considering ways to ethically use such data to fill critical information gaps in women's health research.[6] This Article proceeds in four parts. Part II introduces femtech and the current privacy concerns associated with such apps.

---

[1] *See* 45 C.F.R. § 164.502 (2013).

[2] *See id.*

[3] *See* Celia Rosas, *The Future Is Femtech: Privacy and Data Security Issues Surrounding Femtech Applications*, 15 HASTINGS BUS. L.J. 319, 323 (2019).

[4] *See* Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1785–87 (2021).

[5] The term "femtech" refers broadly to "an expanding category of technology that serves the vast opportunities that exist for female health." *See* Ida Tin, *The Rise of a New Category: Femtech*, CLUE (Sept. 14, 2016), https://helloclue.com/articles/culture/rise-new-category-femtech [https://perma.cc/9T3K-U4XG].

[6] The term "women's health" is inherently exclusionary and fails to reflect the fact that "women's health research is needed by more than just cisgender women[.]" *See* Melissa Nelson et al., *Beyond the Binary: What Does Gender-Inclusive Women's Health Research Look Like?*, WOMEN'S HEALTH RSCH. INST. (Jan. 15, 2020), https://whri.org/beyond-the-binary-what-does-gender-inclusive-womens-health-research-look-like/ [https://perma.cc/CEY8-6YS5]. While gender inclusive language has been developed for clinical care, the research community has not yet adopted research-specific inclusive language. *See id.* This Article uses gendered terms like "women's health" and "femtech" to reflect the language used in cited research while attempting to use inclusive terms where possible and calls on the research community to put more resources toward developing language that is inclusive to all.

Part III discusses the urgent need for stronger, more comprehensive research into women's health issues and explores possibilities for using data collected through femtech apps in such research. Part IV describes the current patchwork of federal laws that provide limited protection for data collected by femtech apps and explores existing proposals for privacy reform in the femtech app space. Lastly, Part V proposes amending the Health Insurance Portability and Accountability Act ("HIPAA") to cover femtech apps, a solution that balances the need for data privacy with the potential to use data from femtech apps to further critical women's health research.

II. BACKGROUND: THE RISE OF FEMTECH AND CURRENT PRIVACY CONCERNS

The femtech market is booming. The term "femtech" was first introduced in 2016.[7] Three years later, "femtech" had secured a place as one of the top ten "words of the year"[8] and the global femtech market was valued at $18.75 billion.[9] Over the next decade, this figure is estimated to reach $50 to $60 billion.[10] Venture capital investment in the femtech industry has grown considerably in recent

[7] *See* Tin, *supra* note 5.

[8] David Shariatmadari, *Cancelled for Sadfishing: The Top 10 Words of 2019*, THE GUARDIAN (Oct. 14, 2019, 3:00 AM), https://www.theguardian.com/science/2019/oct/14/cancelled-for-sadfishing-the-top-10-words-of-2019 [https://perma.cc/VGC7-FMB6] (listing "femtech" as a "key word of the year" alongside others like "pronoun," "nanoinfluencer," and "cancelled").

[9] *Femtech Market by Type, by End-Use, by Application, by Region, Forecasts to 2027*, EMERGEN RSCH. (Aug. 2020), https://www.emergenresearch.com/industry-report/femtech-market [https://perma.cc/MJM6-P8EZ] (predicting an annual growth rate of 15.6 percent, with 36.7 percent of global growth coming from the North American market).

[10] *See id.* (noting that the femtech market is predicted to grow at an annual rate of 15.6% to reach a global market value of $60.01 billion by 2027); *see also Femtech—Time for a Digital Revolution in the Women's Health Market*, FROST & SULLIVAN (Jan. 31, 2018), https://www.frost.com/frost-perspectives/femtechtime-digital-revolution-womens-health-market/ [https://perma.cc/3FPK-V8Z] (predicting that the global market value for femtech will reach $50 billion by 2025).

years.[11] However, there is still significant space for growth as the male-dominated investment world continues to realize the vast potential for profit from an industry whose target market comprises nearly half of the world's population.[12]

While the femtech market includes a variety of technologies that address various aspects of women's health, including menstruation, fertility, pregnancy, menopause, geriatric care, and general wellbeing,[13] a large sector of this market consists solely of menstrual and fertility tracking applications.[14] Femtech apps are mobile apps that "track a user's reproductive cycle, sex life[,] and health in order to provide [users] with algorithmically derived insights into their bod[ies]."[15] More than 100 million individuals use these mobile apps to track their menstrual cycles.[16] In 2016, femtech apps represented the second most popular category of health apps among adolescent

---

[11] *See* Yelena Lavrentyeva, *The Rise of Femtech: Stigma, Market Trends, Challenges, and Opportunities*, ITREX (Apr. 1, 2021), https://itrexgroup.com/blog/femtech-apps-for-women-trends-challenges/ [https://perma.cc/X9PJ-7UTQ].

[12] *See id.* ("There's finally an increasing awareness of huge unmet demand. What were long considered niche needs actually affect roughly half of the global population—a market of 3.73 billion prospective customers."); *see also Population, Female (% of Total Population)*, WORLD BANK (2019), https://data.worldbank.org/indicator/SP.POP.TOTL.FE.ZS [https://perma.cc/3ZP4-BD4G] (estimating that females constitute 49.6% of the global population and 50.5% of the U.S. population).

[13] *See* FROST & SULLIVAN, *supra* note 10.

[14] *See* Laura Shipp & Jorge Blasco, *How Private is Your Period?: A Systematic Analysis of Menstrual App Privacy Policies*, 4 PROC. ON PRIV. ENHANCING TECHS. 491, 491 (2020). While appreciating the breadth of technologies in the femtech sector, this Article focuses primarily on menstrual and fertility tracking apps.

[15] *Id.*

[16] Naomi Kresge, *Period-Tracking Apps Are Monetizing Women's Extremely Personal Data: More Than 100 Million Women Monitor Their Cycles on Their Phones. Here Come the Ads*, BLOOMBERG BUSINESSWEEK (Jan. 28, 2019), https://www.bloomberg.com/news/articles/2019-01-24/how-period-tracking-apps-are-monetizing-women-s-extremely-personal-data [https://perma.cc/7M5Z-DW67].

females and the fourth most popular category of health apps among all adults.[17]

A 2017 study by the U.S. Department of Health and Human Services ("HHS") found that individuals track their cycles for five main reasons: (1) overall bodily awareness; (2) understanding their physical and emotional responses to the different phases of their cycles; (3) feeling prepared for their cycles; (4) planning for pregnancy; and, (5) providing information for conversations with healthcare providers.[18] The difficulties of tracking one's own menstruation and fertility trends are familiar to anyone with a menstrual cycle. From discretely marking calendar days to creating and struggling to keep up with complex spreadsheets, individuals have long been left to their own devices to track this information. On top of these inherent difficulties, historically, many cultures have viewed menstruation as taboo.[19] Menstrual health was "something to only be spoken about in whispers,"[20] and while there are some indications of progress, the societal uncomfortableness surrounding menstrual health remains a reality with serious consequences, including loss of educational opportunities.[21]

---

[17] Michelle L. Moglia et al., *Evaluation of Smartphone Menstrual Cycle Tracking Applications Using an Adapted APPLICATIONS Scoring System*, 127 OBSTETRICS & GYNECOLOGY 1153, 1153 (2016).

[18] Daniel A. Epstein et al., *Examining Menstrual Tracking to Inform the Design of Personal Informatics Tools*, PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 6876, 6879 (2017).

[19] *See Menstruation and Human Rights – Frequently Asked Questions*, U.N. POPULATION FUND (June 2021), https://www.unfpa.org/menstruationfaq [https://perma.cc/44Q6-BTHY]; Marni Sommer & Diana J. Mason, *Period Poverty and Promoting Menstrual Equity*, 2 JAMA HEALTH F. 1, 1 (2021) ("The stigma associated with menstruation perpetuates a culture of silence that may keep the issue hidden from policy makers and others positioned to address it.").

[20] *See FemTech Founder: An Interview with Clue CEO, Ida Tin*, FEMTECH.LIVE (Feb. 11, 2021), https://femtech.live/femtech-founder-an-interview-with-clue-ceo-ida-tin/ [https://perma.cc/BU6L-5H4B].

[21] *See, e.g.*, Sara AlHattab, *Breaking the Cycle of Silence – Menstruation Matters*, UNICEF (May 28, 2019), https://www.unicef.org/jordan/stories/breaking-cycle-silence-menstruation-matters [https://perma.cc/M57H-3W6M]. (explaining that in Jordan, a cultural silence around menstruation causes embarrassment and shame, leading many young girls to remain home from school while menstruating).

Femtech apps provide tools that minimize the inherent difficulty in tracking one's menstruation and fertility.[22] Moreover, femtech apps allow users to take more control over their reproductive and general health, leading to "a greater sense of autonomy[,] which often goes with improved self-worth."[23] Gaining insights into reproductive health is particularly important for people who live in countries where societal pressures and shame prevent young and unmarried women from seeking reproductive health care.[24] Beyond enabling individuals to better understand their bodies, femtech apps provide users with important information to communicate to healthcare providers, supplying clinicians with greater insight into the often-unrecognized patterns and irregularities of reproductive health.[25] In addition to enhancing the depth of the physician-patient relationship, femtech apps have the potential to provide women's health researchers with copious data on reproductive health—an area that has been long under-funded and under-studied.[26]

Despite the promising possibilities for femtech apps to empower women and enhance the medical community's understanding of key women's health issues, femtech apps present significant data privacy concerns. These concerns are, in part, due to the fact that the United States lacks a comprehensive, federal data privacy law.[27] While some states have enacted their own privacy legislation,[28]

---

[22] *See* Alexandra M. Taylor, *Fertile Ground: Rethinking Regulatory Standards for Femtech*, 54 U.C. DAVIS L. REV. 2267, 2297 (2021).

[23] *See id. But see* Epstein, *supra* note 18, at 6882–83 (describing how heteronormative femtech app designs can exacerbate feelings of exclusion for underrepresented groups, e.g., overly feminine design schemes and sexual logging features that assume a male sexual partner).

[24] *See* Fatemeh Mohammadi et al., *The Stigma of Reproductive Health Services Utilization by Unmarried Women*, 18 IRANIAN RED CRESCENT MED. J. 1, 6 (2016).

[25] *See* Taylor, *supra* note 22, at 2297; Johanna Levy & Nuria Romo-Avilés, *"A Good Little Tool to Get to Know Yourself a Bit Better": A Qualitative Study on Users' Experiences of App-Supported Menstrual Tracking in Europe*, 19 BMC PUB. HEALTH 1, 6 (2019).

[26] *See* INST. MED. NAT'L ACADS., WOMEN'S HEALTH RESEARCH: PROGRESS, PITFALLS, AND PROMISE (2010) (ebook), https://www.ncbi.nlm.nih.gov/books/NBK210143/ [https://perma.cc/A7TD-ZBES].

[27] *See* Keats Citron, *supra* note 4, at 1804–05.

[28] *See, e.g.*, *id.* at 1805, 1807–09.

femtech apps remain largely unregulated in terms of data privacy and security.[29]

Concerns about the lack of privacy protections for apps that collect personally identifiable information span across industries and are not limited to femtech.[30] However, an app that collects data on grocery purchasing habits[31] arguably presents less-serious privacy concerns than an app that collects data on a person's sexual history and identifies their peak fertility windows.[32] Although femtech apps have the potential to give women increased control over their reproductive health, the unique nature of the highly personal data collected by femtech apps, coupled with the current lack of federal privacy regulations, presents a strong case for the necessity of heightened protections.

Femtech apps routinely collect data about users' bodies, "particularly the parts of the body associated with sex, gender, sexuality, and reproduction."[33] When app companies sell this information to third parties without users' consent—which they are incentivized to do, given the potential for profit and the lack of regulations to prevent this type of action—they intrude into, what privacy law expert Danielle Keats Citron refers to as, an individual's right to sexual or intimate privacy.[34] Users of femtech apps may

---

[29] *See* Rosas, *supra* note 3, at 323.

[30] *See* Keats Citron, *supra* note 4, at 1817.

[31] *See, e.g.*, *Instacart: Grocery Deliveries*, APPLE APP STORE, https://apps.apple.com/us/app/instacart-grocery-deliveries/id545599256 [https://perma.cc/RG4J-5D5X].

[32] *See, e.g.*, *Period Tracker Period Calendar*, APPLE APP STORE, https://apps.apple.com/us/app/period-tracker-period-calendar/id896501514 [https://perma.cc/YF8B-7CQS]; *Clue Period & Cycle Tracker*, APPLE APP STORE, https://apps.apple.com/us/app/clue-period-cycle-tracker/id657189652 [https://perma.cc/AJF3-7BM8]; *Flo Period & Ovulation Tracker*, APPLE APP STORE, https://apps.apple.com/us/app/flo-period-ovulation-tracker/id1038369065 [https://perma.cc/34ML-R2AF]; *Period Tracker – Eve*, APPLE APP STORE, https://apps.apple.com/tc/app/period-tracker-eve/id1002275138 [https://perma.cc/7BRJ-ML7Z].

[33] *See* Keats Citron, *supra* note 4, at 1768.

[34] *See id.* ("Sexual privacy allows people to set the boundaries around their intimate lives. With sexual privacy, people enjoy sexual autonomy. They get to decide who learns about their innermost fantasies, sexual history, and sexual and reproductive health."); *id.* at 1793; *see also* Griswold v. Connecticut, 381 U.S.

share general health-related data, like their weight, mood, activity levels, or smoking habits, along with much more sensitive and intimate data like menstrual irregularities, bodily secretions, sexual activity, sexual desires, and history of sexual assault, miscarriages, abortions, and more.[35] Additionally, some femtech companies are now pairing apps with data-tracking devices, like digital menstrual cups, vaginal thermometers, and portable ultrasound devices.[36]

Unfortunately, many femtech app users are not aware that the personal data they share is essentially unprotected.[37] In a 2020 study, researchers at the Health Law and Policy Institute found that none of the fifteen most popular menstrual-tracking apps required users to view the apps' terms of service or privacy policies prior to use.[38] Additionally, users who did access these documents needed a college-level education to read (let alone, fully comprehend) the average app's terms of service and privacy policies.[39] Nevertheless, many users of menstrual-tracking apps assume that their data is kept private.[40]

The lack of privacy and security protections poses serious consequences for users of femtech apps, and it is becoming increasingly clear that data collected by femtech apps have not been safeguarded in ways that meet users' assumptions. To start, femtech

---

479, 485–86 (1965) (recognizing a fundamental right to privacy in intimate marital decisions); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (extending the fundamental right to intimate privacy recognized in *Griswold* to unmarried people and noting that, "[i]f the right of privacy means anything, it is the right of the individual . . . to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child"); Roe v. Wade, 410 U.S. 113, 153–54 (1973) (holding that a woman has a fundamental, albeit qualified, right to make personal reproductive health decisions).

[35] *See* Keats Citron, *supra* note 4, at 1775–77.

[36] *Id.* at 1777; Bob Kronemyer, *Femtech Health Technology Takes Center Stage*, CONTEMP. OB/GYN 23, 23 (2018).

[37] *See* Leah R. Fowler et al., *Readability and Accessibility of Terms of Service and Privacy Policies for Menstruation-Tracking Smartphone Applications*, 21 HEALTH PROMOTION PRAC. 679, 680–81 (2020).

[38] *Id.*

[39] *Id.* at 681.

[40] *See id.* at 680 (stating that femtech app users often erroneously assume that the data they use these apps to track is kept private).

app companies often sell user data to third parties, which in turn sell that information to data aggregators or brokers.[41] A recent study of ten popular femtech apps found that those apps sold user data to over 135 companies, including Facebook and Amazon, as well as firms specializing in targeted advertisements.[42] Shockingly, there have even been instances of employers gaining access to their employees' data from femtech apps.[43] Without femtech app users' knowledge, their intimate data is used to "train algorithms used in hiring, housing, insurance, and other crucial decisions."[44] Such algorithms can predict that an individual may need costly fertility treatments or may consider undergoing gender confirmation surgery in the future, potentially increasing that individual's insurance premiums.[45] Further, the negative personal outcomes that arise when femtech app developers sell user data to third parties may be felt disproportionately by women, non-white people, and the LGBTQ community.[46] Putting intimate personal data into the hands of private parties without user consent deprives individuals of the autonomy to control who may access the most intimate details of their lives.[47]

Several recent examples illustrate the serious consequences that can occur when femtech apps are left unregulated. First, a *Wall Street Journal* investigation found that Flo Health, maker of the *Flo Period & Ovulation Tracker*, repeatedly profited through supplying third parties, including Google and Facebook, with unrestricted use of its users' intimate, personal data.[48] Data sold to third parties included dates of a user's menstrual cycles, as well as whether and when a user was attempting to conceive.[49] One can imagine why any person, especially one who has suffered a miscarriage or undergone an abortion, might not want to receive targeted advertisements using

---

[41] *See* Keats Citron, *supra* note 4, at 1799.
[42] *See id.* at 1805.
[43] *See id.* at 1798.
[44] *Id.* at 1799.
[45] *See id.* at 1770.
[46] *See id.* at 1796 (noting that while white men are often celebrated for their sexual activities and desires, "women, racial minorities, and LGBTQ individuals are stigmatized, marginalized, and disempowered").
[47] *Id.* at 1793.
[48] *See* Complaint, In re Flo Health, Inc., Docket No. 1923133, ¶ 5.
[49] *See* Keats Citron, *supra* note 4, at 1777.

that data. Another femtech app, *FEMM*, a self-described "new revolution in women's health" that "uses cutting edge science," was created by an anti-abortion advocacy group.[50] Consequently, *FEMM* advises its users that taking birth control is unsafe and discourages them from seeking abortions, regardless of medical necessity.[51] However, information about the company's anti-abortion stance is not affirmatively disclosed to users.[52]

Additionally, a recent Consumer Reports investigation uncovered several security threats to user data on the popular *Glow* app.[53] Consumer Reports found a number of "surprising vulnerabilities" that could allow "stalkers, online bullies, or identity thieves to use the information they gathered to harm *Glow*'s [four million] users."[54] Perhaps most alarmingly, anyone who knew a *Glow* user's email address—whether a "loving partner, obsessive ex-husband, or anonymous creep"—could link accounts without that user's permission or knowledge.[55] By simply requesting to link accounts, any person could immediately gain access to the user's data, "including the dates of abortions and sexual encounters."[56] The investigation uncovered another disconcerting vulnerability through which anyone who downloaded free, easy-to-use software could click on any *Glow* user's posts to one of the app's forums and access

---

[50] *See id.* at 1803.

[51] *See id.* at 1804.

[52] *See id.*

[53] *See* Jerry Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds*, CONSUMER REPS. (Sept. 17, 2020), https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats-a1100919965/ [https://perma.cc/M69G-Q8K9]; *see also Glow Period, Fertility Tracker*, APPLE APP STORE, https://apps.apple.com/us/app/glow-period-fertility-tracker/id638021335 [https://perma.cc/P3JU-77TR] (describing *Glow* as a fertility and period tracker that aids in conception and gives users control over their reproductive health by recording information on basal body temperature, cervical mucus, menstrual flow, pregnancy test results, sexual activity, height, weight, sleep patterns, and more).

[54] Beilinson, *supra* note 53.

[55] *See id.* (noting that a request to link accounts is sent to the user, but no action is required on her part; therefore, if the request email ends up in her spam folder or if she never opens it, the requesting party has automatic access to much of her data).

[56] *See* Keats Citron, *supra* note 4, at 1777.

that user's name, email address, approximate location, "and a number of details from her health log."[57] Following the Consumer Reports investigation, *Glow* updated its app to address all of these vulnerabilities and notified users about the updates.[58] While *Glow*'s security issues are alarming, perhaps they are not surprising given that Hard Valuable Fun ("HVF"), the developer of *Glow* and other femtech apps, describes one of its objectives as "tak[ing] advantage of . . . *high storage capacity to collect and explore data as a commodity*."[59] The current paucity of data privacy laws serves only to encourage this type of profit-seeking behavior, leaving app users with little to no recourse, aside from choosing not to use femtech apps.[60]

III. PROMISING CAPABILITIES: THE POTENTIAL FOR DATA COLLECTED BY FEMTECH APPS TO FILL CRITICAL WOMEN'S HEALTH RESEARCH GAPS

The potential for femtech apps to provide individuals and healthcare providers with more information about women's health is valuable, given the historical lack of focus and funding directed toward women's health research in the United States.[61] Women have been chronically underrepresented in studies of disease progression and treatment, leaving healthcare providers uncertain regarding how best to predict risk and prescribe proper treatment to female patients.[62] Today, approximately one-third of women in the United States have used a femtech app during their lifetime.[63] In 2016, seven-percent of the apps available to download in Apple's App Store were femtech apps.[64] With such widespread use, femtech apps have the potential to provide a novel source of aggregated data on reproductive health that could benefit public health research and improve women's health outcomes.

---

[57] *See* Beilinson, *supra* note 53.
[58] *See id.*
[59] *See* Keats Citron, *supra* note 4, at 1777; *see also* Beilinson, *supra* note 53.
[60] *See* Keats Citron, *supra* note 4, at 1767.
[61] *See* INST. MED. NAT'L ACADS., *supra* note 26.
[62] *See* Anna Nowogrodzki, *Inequality in Medicine*, 550 NATURE S18 (2017).
[63] Keats Citron, *supra* note 4, at 1775.
[64] *See* Moglia et al., *supra* note 15, at 1153.

A. Women Are Critically Underrepresented in Medical Research

Until the 1970's, women were excluded from clinical trials in the United States because of the widespread belief throughout the medical community that their menstrual cycles could bias study results in unpredictable ways that could not be statistically adjusted.[65] The federal government has undertaken efforts in recent years to increase the number of women included in public health research.[66] Despite these efforts, women remain underrepresented, particularly in studies of disease progression and treatment.[67] For example, only one-third of participants in cardiovascular clinical trials are women, despite the fact that cardiovascular disease is the leading cause of death for American women.[68] Furthermore, the under-inclusion of women in research begins before the clinical trial phase; preclinical drug trials in animals are heavily biased toward males.[69] Some animal studies include no females at all, while others report a male-to-female ratio of sixteen-to-one.[70] As Georgetown University researcher Kathryn Sandberg notes, this "bias[es] the whole drug pipeline toward what is optimal in the male."[71]

As more women have been included in clinical studies over the years, significant sex differences have emerged—differences in drug reactions, pain processing, and risk factors for certain diseases.[72] For example, studies including women have revealed significant sex-based differences in the prevalence of and treatment for cardiovascular disease, lung cancer, depression, and Alzheimer's disease.[73] However, even when women are included in clinical trials, many studies do not separately analyze data by sex or report any

---

[65] *See* Ruth B. Merkatz, *Inclusion of Women in Clinical Trials: A Historical Overview of Scientific, Ethical, and Legal Issues*, 27 J. OBSTETRIC, GYNECOLOGIC & NEONATAL NURSING 78, 78–79 (1998).

[66] *See* Paula A. Johnson et al., *Sex-Specific Medical Research: Why Women's Health Can't Wait*, MARY HORRIGAN CONNORS CTR. WOMEN'S HEALTH & GENDER BIOLOGY BRIGHAM WOMEN'S HOSP. 1, 5 (2014).

[67] *See id.*; *see also* Nowogrodzki, *supra* note 62, at S18.

[68] *See* Johnson, *supra* note 66, at 5, 12.

[69] *See* Nowogrodzki, *supra* note 62, at S18–19.

[70] *See id.* at S19.

[71] *See id.*

[72] *See id.*

[73] *See* Johnson, *supra* note 66, at 5.

sex-based differences in their results.[74] Additionally, many pharmaceuticals are less effective in women, and women are more likely to experience adverse drug-related reactions.[75] Nonetheless, the U.S. Food and Drug Administration ("FDA") does not require sex-specific data analyses from drug trials before making dosing recommendations.[76]

The under-inclusion of women in medical research has left healthcare providers without comprehensive—or even adequate—data regarding women's health, limiting their ability to provide high-quality, evidence-based care.[77] Providers face critical gaps in their understanding of how to best prevent and treat many diseases and illnesses prevalent in women patients.[78] In addition to the "deeply rooted" underrepresentation of women in medical research,[79] a history of political resistance against women's reproductive agency, along with reproductive health taboos, has caused major gaps in knowledge about reproductive health.[80]

B. Data Collected by Femtech Apps Can Fill Critical Research Gaps

Given these persisting gaps in medical knowledge about women's health, femtech apps have the potential to provide healthcare professionals with unprecedented amounts of data to advance critical insights into women's health. The ease and convenience of using an app to collect data (as opposed to visiting a research site) may allow for the inclusion of women who would

---

[74] *See id.* at 8; *see also* Nowogrodzki*, supra* note 62, at S18 (noting that only 31% of cardiovascular clinical trials stratify their results by sex).

[75] *See* Nowogrodzki, *supra* note 62, at S18 (explaining that between 1997 and 2000, 80% of drugs removed from the U.S. pharmaceutical market were removed due to adverse effects in women).

[76] *See* Johnson, *supra* note 66, at 8.

[77] *See id.* at 5.

[78] *See* Nowogrodzki, *supra* note 62, at S18.

[79] *Id.*

[80] *See* Clara Moskowitz, *Fertile Ground: The Long-Neglected Science of Female Reproductive Health*, SCI. AM. (May 1, 2019), https://www.scientificamerican.com/article/fertile-ground-the-long-neglected-science-of-female-reproductive-health/ [https://perma.cc/4MRH-WAM7].

otherwise be unable to participate in clinical research studies.[81] Apart from clinical trials, the large number of women who use femtech apps presents the opportunity for large-scale observational studies of important reproductive health trends.[82]

Research on the recently developed COVID-19 vaccine provides an illustrative example of the potential of femtech apps to fill knowledge gaps that arise when researchers fail to consider women's health outcomes.[83] After receiving a COVID-19 vaccine, numerous individuals used social media to chronicle temporary changes to their menstrual cycles.[84] However, none of the clinical trials for the COVID-19 vaccines collected data about the relationship between vaccination and menstruation.[85] Furthermore, HHS's online system for reporting adverse events associated with COVID-19 vaccination did not collect any information about menstrual cycle outcomes.[86] This lack of data has left healthcare providers unable to properly advise patients about any menstrual changes they might expect post-vaccination.[87] To begin to fill this research gap, a forthcoming study funded by the National Institutes of Health ("NIH") used data collected through the femtech app, *Natural Cycles*, to analyze the correlation between COVID-19

---

[81] *See* Nicole Wetsman, *Data from Health Apps Offers Opportunities and Obstacles to Researchers*, VERGE (July 3, 2019, 3:09 PM), https://www.theverge.com/2019/7/3/20681254/data-health-apps-clue-period-tracking-sleep-fitness-research [https://perma.cc/M6H2-6JMP].

[82] *See, e.g.*, Anna Druet, *Scientific Research at Clue: How Tracking Your Cycle Advances Female Health*, CLUE (Mar. 27, 2018), https://helloclue.com/articles/about-clue/scientific-research-at-clue [https://perma.cc/H34P-AMRB] (describing a collaboration between the *Clue* app and researchers at Columbia University as, "in essence[,] the largest observational study about menstrual health . . . [that] will shed new light on the menstrual cycle and its phenotypic variations").

[83] *See* Alison Edelman et al., *Association Between Menstrual Cycle Length and Coronavirus Disease 2019 (COVID-19) Vaccination*, OBSTETRICS & GYNECOLOGY (forthcoming 2022) (manuscript at 1–2).

[84] *See id.* at 2.

[85] *Id.*

[86] *See id.*

[87] *Id.*

vaccination and menstrual cycle disturbances.[88] The *Natural Cycles* study found that, although vaccination was occasionally associated with a longer menstrual cycle, this change was temporary and not "clinically meaningful."[89] This study highlights the potential to use data collected through femtech apps to support research into women's health outcomes that are too often overlooked. Consequently, any proposal to strengthen privacy protections for data collected by femtech apps should also consider how to incorporate the possibility of giving users the ability to opt into research studies while keeping their data protected.

IV. THE NEED FOR STRONGER LEGAL PROTECTIONS OF PERSONAL DATA COLLECTED BY FEMTECH APPS

In today's increasingly digital world, mobile applications constantly collect data about all aspects of human life. Public concern about how this data is used and sold is intensifying, accompanied by demands for comprehensive data privacy legislation.[90] Data collected by femtech apps raise heightened concerns about privacy because these apps track a unique mix of highly-sensitive data, including general and reproductive health information and users' sexual practices.[91] Despite the intimate, personal nature of data collected by and stored on femtech apps, few laws protect the privacy and security of such data in the United States.[92]

Three federal agencies have limited regulatory authority over femtech apps regarding data privacy and security—the Federal Trade Commission ("FTC"), the FDA, and the HHS. However, all

---

[88] *See id.* ("Individuals who use . . . *Natural Cycles* voluntarily choose to prospectively track physiologic data related to their menstrual cycles for purposes of nonhormonal pregnancy prevention or planning and consent to the use of their de-identified data for research (consent can be removed if desired)."). The *Natural Cycles* app prompted users to enter their COVID-19 vaccination status and corresponding dates of vaccination. *See id.* If app users did not enter this information, they were excluded from the study. *Id.*

[89] *See id.* at 8.

[90] *See* Keats Citron, *supra* note 4, at 1838.

[91] *See* Shipp & Blasco, *supra* note 14, at 491.

[92] *See* Keats Citron, *supra* note 4, at 1804.

three agencies have narrow authority to regulate only certain apps or activities. This assortment of inadequate federal oversight leaves many femtech apps completely unregulated when it comes to how the apps store, use, and share personal data. In addition to federal regulations, some states have unilaterally passed laws that provide stronger privacy and security protections.[93] This patchwork of federal and state laws has led to confusion about the laws with which femtech app makers must comply and leaves users in the dark about the safety of their personal reproductive health information. Given these concerns, several legal scholars have described proposals for strengthening privacy protections for data collected by apps in the rapidly expanding femtech market.[94]

A. Current Federal Privacy Laws Regulating Femtech Apps

First, femtech apps are subject to FTC oversight.[95] Section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[96] In practice, the FTC Act prohibits femtech app companies from "mislead[ing] consumers about what is happening with their health information."[97] To comply, the FTC discourages app companies from burying any privacy information in a way that makes it difficult for consumers to understand or providing consumers with contradictory information about data privacy.[98] Additionally, the FTC's Health Breach Notification Rule ("HBNR") requires femtech apps to notify users if any data breach occurs involving their personal information.[99] Importantly, however, the FTC Act merely ensures that users receive notice about an app provider's data policies and any breaches of those policies regarding the storing or usage of user's data, but the Act does not, in fact,

---

[93] *See* Rosas, *supra* note 3, at 336.

[94] *See, e.g.*, Taylor, *supra* note 22; Rosas, *supra* note 3; Keats Citron, *supra* note 4.

[95] *See* Rosas, *supra* note 3, at 323.

[96] 15 U.S.C. § 45(a) (2006).

[97] *Sharing Consumer Health Information? Look to HIPAA and the FTC Act*, FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act [https://perma.cc/2Z3P-GNQC].

[98] *See id.*

[99] *Id.*; *see also* 16 C.F.R. § 318 (2009). The HBNR also requires an app company to notify the media of any breach involving 500 or more consumers. *Id.*

provide any meaningful protection for a user's information.[100] Furthermore, FTC enforcement in the femtech app industry has thus far been extremely limited.[101]

Second, the FDA, which is statutorily obligated to protect public health, has regulatory authority over medical devices, including mobile medical apps ("MMAs").[102] However, the Agency has taken a largely "hands-off" approach to regulating femtech apps based on the way the Agency classifies risks posed by MMAs.[103] Typically, the FDA categorizes medical devices into "classes" based on the level of public health risk involved—i.e., as the level of risk increases, so too does the degree of regulatory control required.[104] However, before placing MMAs into one of the traditional risk "classes," the FDA places these apps into two categories: (1) apps that turn smartphones into medical devices and therefore may pose risks to users "if they function improperly," and (2) apps that may be classified as "medical devices" but nonetheless pose only a low or moderate risk to users.[105] If an MMA is in the first category, it is placed into a risk-based "class" and is subject to full FDA

---

[100] *See* Rosas, *supra* note 3, at 334 (asserting that the FTC Act does not provide adequate privacy and security protections for femtech apps in part because the Act "does not regulate the manners, mechanisms, and means of how a company's technological infrastructure must operate to ensure consumer's privacy rights are upheld").

[101] *See* F.T.C., Joint Statement of Comm'r Rohit Chopra and Comm'r Rebecca Kelly Slaughter: *In re Flo Health, Inc.* Comm'n File No. 1923133 at 1 (Jan. 13, 2021) (remarking that the FTC's proposed complaint against Flo Health did not include a violation of the HBNR when the Agency had the authority to do so and calling for more stringent enforcement utilizing all of FTC's available enforcement mechanisms).

[102] *See* Taylor, *supra* note 22, at 2277, 2280.

[103] *See id.* at 2270, 2277.

[104] *See Classify Your Medical Device*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device [https://perma.cc/6GRG-6JW2] (stating Class I devices pose the lowest risk and are subject to the least regulation, while Class III devices have the highest level of risk and are subject to the strictest regulations); *see also* Taylor, *supra* note 22, at 2270, 2277.

[105] *See* Taylor, *supra* note 22, at 2281 (noting that apps which primarily "offer patient education or serve as reference aids" are deemed to pose only a low to moderate risk to public health).

regulation.[106] However, if an MMA falls in the second category, it is only subject to the FDA's "enforcement discretion," as opposed to full agency regulation.[107] Despite the fact that many femtech apps pose significant risks to users if they function improperly (e.g., by providing inaccurate fertility predictions leading to unplanned pregnancies),[108] the FDA has failed to exercise regulatory authority over most of these apps.[109]

This lack of FDA regulation is not accidental; through recent legislation, Congress sought to decrease the "regulatory burdens" associated with app development in an effort to drive marketplace innovation and technological advancement, and FDA guidance reflects these goals.[110] The 21st Century Cures Act ("Cures Act") along with the 2017 Digital Health Innovation Action Plan ("Innovation Plan") make clear that the FDA will only regulate "high-risk MMAs" as medical devices.[111] The shared aim of the Cures Act and the Innovation Plan is to promote mobile health innovation, allowing apps to reach the market faster.[112] One result of this goal is the FDA's hands-off approach to regulating femtech apps.[113]

Third, HHS is tasked with enforcing HIPAA, which was enacted in 1996[114]—well before smartphones or data-collecting apps were

---

[106] *See id.*

[107] *See id.*

[108] *See id.* at 2276 (describing an investigation of the *Natural Cycles* app in Sweden, which found that at least 676 of the apps' users had unintended pregnancies and thirty-seven users sought abortions at a single clinic during a four-month period).

[109] *See id.* at 2283–86.

[110] *See id.* at 2280–83.

[111] *See id.* at 2281–83 ("The Digital Health Innovation Action Plan and the [21st Century] Cures Act together reflect the fundamental tension between the FDA's core responsibilities. The Agency must balance the need for innovation and efficiency in the approval process with the need to provide patients with treatment options that are backed by proven safety and efficacy data.").

[112] *See id.*

[113] *See id.*

[114] *Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS., (2003).

ubiquitous.[115] As a part of the Social Security Act, HIPAA was originally enacted to protect individuals who lose or change employment from simultaneously losing all healthcare coverage.[116] Title II of HIPAA requires HHS to promote efficiency in the storage and transmission of patient data or protected health information ("PHI") and, to this end, encourages PHI to be stored electronically.[117] Title II also includes HIPAA's Privacy Rule, Security Rule, and Breach Notification Rule.[118] HHS's Office of Civil Rights ("OCR") is responsible for enforcing these rules.[119] Thus, even though HIPAA is not a privacy bill *per se*, the Act has developed to provide expansive privacy protections for PHI.[120] Unfortunately, however, most femtech apps are not required to comply with HIPAA's privacy and security regulations.[121]

HIPAA defines PHI as "individually identifiable health information" in any form (including electronic) that is maintained or transmitted by a covered entity.[122] "Individually identifiable health information" includes any data related to someone's "past, present[,] or future physical or mental health condition."[123] Although many femtech apps regularly collect "individually identifiable

---

[115] *See, e.g.*, *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/T3HX-KB6A] (citing data from Pew Research Center's first smartphone ownership survey in 2011, fifteen years after HIPAA was first enacted, which found that only thirty-five percent of U.S. adults owned a smartphone, compared to eighty-five percent of U.S. adults in 2020); Matt Strain, *1983 to Today: A History of Mobile Apps*, GUARDIAN (Feb. 13, 2015, 6:00 EST), https://www.theguardian.com/media-network/2015/feb/13/history-mobile-apps-future-interactive-timeline [https://perma.cc/F55S-K3Z5] (noting that, while early PDAs like the Nokia 6110 had built in games like 'Snake,' the modern app emerged when Apple introduced the first 500 apps in 2008).

[116] *See* Donna Bowers, *The Health Insurance Portability and Accountability Act: Is It Really All That Bad?*, 14 PROC. BAYLOR UNIV. MED. CTR. 347, 347 (2001).

[117] *See id.*

[118] *See id.*

[119] *See* 45 C.F.R. § 160.

[120] *See* Keats Citron, *supra* note 4, at 1806.

[121] *See* Rosas, *supra* note 3, at 323.

[122] *See* 45 C.F.R. § 160.103.

[123] *See id.*

health information,"[124] most smartphone apps do not meet HIPAA's narrow definition of "covered entity."[125] HIPAA applies to three categories of entities: (1) health plans; (2) health plan clearinghouses; and, (3) healthcare providers that electronically transmit certain PHI, and also applies to the business associates of any covered entity.[126] A small number femtech apps are considered business associates of covered entities and are therefore subject to HIPAA compliance.[127] For example, the *Glow* app allows its users to participate in a program through which the app communicates fertility information between patients and healthcare providers.[128] *Glow* is thus considered a business associate under HIPAA and must comply with certain privacy and security regulations.[129] To the contrary, any femtech app not considered a business associate of a covered entity falls outside the regulatory scope of HIPAA.[130]

B. Strengthening Privacy Protections: Existing Proposals for Reform

The uniquely intimate nature of the data collected by femtech apps poses distinct risks to users.[131] These risks accordingly call for unique legal solutions. As femtech apps grow in popularity, so do concerns over how app developers are using and could use this data at the expense of their users.[132] Legal scholarship focusing on this issue is new and developing. Some proposed solutions suggest amending or expanding current federal laws to provide greater privacy protections.[133] Additionally, federal and state lawmakers have recently proposed legislation addressing certain aspects of data

---

[124] *See* Rosas, *supra* note 3, at 329 (noting that "[f]emtech mobile applications and medical records often contain the same level of personal health information").

[125] *See id.* at 323.

[126] *See id.*

[127] *See id.* at 325–26.

[128] *See id.* (describing the "Glow Fertility Program Patient Services Agreement").

[129] *See id.*

[130] *See id.* at 322–23.

[131] *See* Fowler et al., *supra* note 37, at 680.

[132] *See, e.g.*, Taylor, *supra* note 22; Rosas, *supra* note 3; Keats Citron, *supra* note 4.

[133] *See, e.g.*, *id.*

privacy, and federal agencies have begun to exercise enforcement over femtech apps in response to egregious privacy violations.[134] Below are several suggestions for how current and proposed federal laws could strengthen data privacy protections for femtech app users, along with potential challenges and drawbacks to each approach.

1. Using Existing Enforcement Mechanisms Under the FTC

The FTC could exercise greater enforcement control over femtech apps under the FTC Act, which prohibits companies that collect health-related data from "mislead[ing] consumers about the companies' privacy and data security policies" related to PHI.[135] A groundbreaking FTC action against a popular femtech company, Flo Health, Inc. ("Flo Health"), illustrates that the FTC may be willing to hold femtech companies accountable for failing to provide notice to users before disclosing their data to third parties.[136] Additionally, a recent FTC policy statement makes clear that the Agency will increase enforcement of its HBNR, specifically as the Rule applies to apps that collect health data.[137]

In January 2021, the FTC ordered Flo Health, a femtech company that advertises and sells the *Flo Period & Ovulation Tracker* ("*Flo App*"),[138] to notify its users that their data had been shared with third parties without their knowledge or consent.[139] According to the FTC complaint, millions of women who use the *Flo App*[140] entrusted Flo Health with their intimate reproductive

---

[134] *See Keats Citron*, *supra* note 4, at 1807–10; *see also* Revisiting the Need for Federal Data Privacy Legislation, Hearing Before the Comm. on Commerce, Science, and Transportation, 116th Cong. (Sept. 23, 2020).

[135] *See* Rosas, *supra* note 3, at 323, 334.

[136] *See* Complaint, In re Flo Health, Inc., Docket No. 1923133.

[137] *See* F.T.C., Statement of the Commission on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021).

[138] *See* Complaint, In re Flo Health, Inc., Docket No. 1923133, ¶ 2.

[139] *See* F.T.C., Joint Statement of Comm'r Rohit Chopra and Comm'r Rebecca Kelly Slaughter In re Flo Health, Inc., Comm'n File No. 1923133, at 1 (Jan. 13, 2021) (concurring in part, dissenting in part).

[140] *See* Complaint, In re Flo Health, Inc., Docket No. 1923133, ¶ 9 (identifying that Flo App users include over 16 million users in the U.S. and that the Flo App was the Apple App Store's "most downloaded app" in 2019).

health data.[141] Flo Health's privacy policies repeatedly stated that the app would not share users' health information with anyone and "would only use *Flo App* users' data to provide the *Flo App's* services."[142] However, for several years, Flo Health provided a number of third parties (such as Google and Facebook) with unrestricted access to user data, including information about menstruation, fertility, and childbirth.[143] The FTC charged Flo Health with seven counts of misrepresentation in violation of the FTC Act.[144] Flo Health reached a settlement with the FTC in June of 2021.[145] Under the settlement terms, Flo Health is now required to notify all affected app users about the disclosure of their health data.[146] Flo Health must undergo an independent review of its privacy policies, and, going forward, the company will have to obtain users' affirmative consent before sharing any data with third parties.[147] This significant action suggests that the FTC may be more willing in the future to hold similar femtech app companies accountable for selling or disclosing user data without their consent. At a minimum, this action signals to other femtech app companies that they should take care to protect their users' information or, at the very least, request consent from their users prior to disclosing health data to third parties.

After the FTC filed its complaint against Flo Health, two FTC Commissioners, Rohit Chopra and Rebecca Kelly Slaughter, filed a Joint Statement, concurring with the FTC's action but expressing disappointment that the Agency failed to employ all of its available

---

[141] *See id.* ¶ 3.

[142] *See id.* ¶ 13.

[143] *See id.* ¶¶ 3–6 (noting that Flo Health did nothing "to limit what these companies could do with the users' information[,]" thereby giving third parties unrestricted access to "use Flo App users' personal health information expansively, including for advertising").

[144] *See id.* ¶¶ 56–65.

[145] *See 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/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared [https://perma.cc/C94A-YY2E].

[146] *See id.*

[147] *See id.*

enforcement mechanisms.[148] Specifically, the Commissioners argued that, in addition to FTC's unprecedented privacy action against Flo Health, the Agency should have held Flo Health accountable for violating the HBNR, "one of only a handful of federal privacy laws protecting consumers."[149] The HBNR requires mobile health apps ("mHealth apps") that collect personal health data to notify users of any unauthorized data disclosures.[150] However, as the Commissioners critically noted, the FTC has never brought an action to enforce this Rule.[151]

Perhaps in response to Chopra and Slaughter's Joint Statement, the FTC released a policy statement on September 15, 2021, to provide guidance, clarify misunderstandings, and notify mHealth apps about the scope and requirements of the HBNR.[152] In its statement, the FTC noted that the HBNR is increasingly important given "the proliferation of apps and connected devices that capture sensitive health data."[153] The statement clarified that, although apps are only subject to the Rule if they create a "personal health record" with data drawn from "multiple sources," the FTC interprets this requirement broadly to cover most health apps.[154] The FTC further illuminated that a "breach" under the HBNR includes any unauthorized sharing of an app user's health data and "is not limited to cybersecurity intrusions or nefarious behavior."[155] Finally, the FTC warned that the Agency intends to bring enforcement actions

---

[148] *See* F.T.C., Joint Statement of Comm'r Rohit Chopra and Comm'r Rebecca Kelly Slaughter *In re Flo Health, Inc.*, Comm'n File No. 1923133, at 1 (Jan. 13, 2021) (concurring in part, dissenting in part).

[149] *See id.* at 1–2.

[150] *Id.* at 2.

[151] *See id.* at 3 (suggesting that the FTC should use all of its available authority to prevent data abuse and stating that the HBNR "will have its intended effect only if the FTC is willing to enforce it").

[152] *See* F.T.C., Statement of the Comm'n on Breaches by Health Apps and Other Connected Devices, at 1 (Sept. 15, 2021).

[153] *See id.*

[154] *See id.* at 2 (clarifying that an app meets the "multiple sources" requirement if it (1) draws personal health data from user input and has the ability to sync with a user's fitness tracker or (2) only draws health information from one source, "but also takes non-health information from another source (e.g., dates from your phone's calendar)").

[155] *See id.*

against mHealth apps under the HBNR for any violations that will result in "civil penalties of $43,792 per violation per day."[156] Hopefully, the threat of such substantial penalties will lead femtech app developers to rethink their privacy policies.

While heartening that the FTC has recently recognized the importance of holding mHealth apps more accountable than the Agency has been willing to do in the past, the FTC's regulatory authority remains too limited, given the extremely sensitive nature of data collected by femtech apps. The FTC could require femtech apps to develop informative privacy policies and ensure users are notified if a data breach occurs. However, the Agency's authority is limited to bringing enforcement actions only after a breach occurs,[157] at which point—particularly from the app user's perspective—the damage has already occurred. While the FTC's settlement with Flo Health required the company to "instruct any third party that received users' health information to destroy that data[,]" the settlement provides little solace for app users with no knowledge as to how their reproductive health data was used and no assurance regarding if or when their data will be destroyed.[158]

2. Regulating Certain Femtech Apps as "Medical Devices" Under the FDA

Although the FDA currently regulates only femtech apps that pose significant risks to users, its recent action indicates it might be possible to bring more femtech apps under full FDA regulation.[159] Rapid technological advancements in femtech app development, like the ability to take internal body temperatures and predict fertile and non-fertile windows as a means of contraception, make these apps more likely to pose risks to users if the apps function

---

[156] *Id.*

[157] *See* 16 C.F.R. §§ 318.3(a), 318.7 (2022).

[158] *See FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, U.S. FED. TRADE COMM'N (June 22, 2021), https://www.ftc.gov/news-events/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared [https://perma.cc/C94A-YY2E].

[159] *See* Taylor, *supra* note 22, at 2281.

improperly.[160] For example, in 2018, *Natural Cycles* became the first femtech app to obtain FDA approval as a digital contraceptive.[161] As part of the Agency's approval process, the FDA created a new category of medical devices subject to regulatory control, called Software Applications for Contraception ("SACs").[162]

The FDA defines SACs as apps that algorithmically analyze user data (e.g., internal temperature and dates of menstruation) to provide personalized fertility predictions for contraceptive purposes.[163] SACs are categorized as "moderate risk" devices, which subjects them to certain device-specific regulatory controls, including "performance standards, postmarket surveillance, and premarket data requirements."[164] Several femtech apps currently give personalized fertility predictions and are advertised as contraceptives,[165] meaning the apps fall within the FDA's definition of SACs and, following the example of *Natural Cycles*, should be subject to full FDA regulation as "medical devices."[166]

While classifying more apps as SACs could expand FDA regulation in the femtech market, this approach has several limitations. First, the FDA's regulatory controls primarily focus on the public health risks inherent in apps that purport to tell users if and when they might become pregnant.[167] To be clear, as an agency charged with protecting public health, the FDA's regulations

---

[160] *See id.* at 2283–86 ("While [some femtech] apps do have 'low risk' features that serve to educate women about their menstrual cycles or allow them to monitor their personal health data, they are undeniably marketed and meant to be used as contraceptives . . . .").

[161] *See id.* at 2270. *Natural Cycles* is a femtech app that is advertised as a contraceptive and analyzes user input data to predict "fertility status." *See id.* at 2269, 2276.

[162] *Id.* at 2279–80.

[163] *Id.* at 2278.

[164] *Id.* at 2270, 2279.

[165] *See id.* at 2283 (suggesting that unregulated femtech apps including *Flo*, *Dynamic Optimal Timing*, and *Ovia* meet the definition of SACs and should be regulated by the FDA).

[166] *See id.* at 2283, 2285–86 ("While these apps do have 'low risk' features that serve to educate women about their menstrual cycles or allow them to monitor their personal health data, they are undeniably marketed and meant to be used as contraceptives just like Natural Cycles.").

[167] *See id.* at 2278.

correctly focus on health risks instead of privacy concerns.[168] While the FDA should undoubtedly subject fertility-predicting femtech apps to full regulatory control, FDA regulation falls short of the type of stringent privacy protections needed to protect the data collected by femtech apps. Additionally, based on current FDA policy, this approach only applies to apps that meet the definition of SACs, leaving out all other femtech apps that may nonetheless collect sensitive user data (e.g., apps that track menstruation and/or sexual activity but do not give specific contraceptive advice).[169] While FDA regulation is an important step in regulating health risks posed by a segment of femtech apps,[170] the limits of the Agency's authority leave many apps unregulated by focusing on risks to public health rather than risks to privacy.

3. Expanding the Definition of "Covered Entity" Under HIPAA

The best avenue for expanding current privacy protections to cover data collected by femtech apps is to amend the statutory definition of "covered entity" under HIPAA. If HIPAA were amended to include femtech apps as covered entities, user data would be protected under HIPAA's Privacy Rule, Security Rule, and Breach Notification Rule. The Privacy Rule outlines how a covered entity may use or disclose PHI.[171] The Privacy Rule enumerates a limited number of exceptions in which a covered entity may be permitted to disclose PHI (e.g., to another healthcare provider if the disclosure is related to treatment or payment).[172] Aside from these narrow permissive uses, however, a covered entity is prohibited from disclosing an individual's PHI without obtaining written authorization.[173] Even so, the Privacy Rule mandates that

---

[168] *See id.* at 2277 (noting that "[t]he FDA's responsibility to protect public health underlies its overall approach to testing and regulating medical devices, including SACs").

[169] *See, e.g.*, *Period Tracker by GP Apps*, APPLE APP STORE, https://apps.apple.com/us/app/period-tracker-by-gp-apps/id330376830 [https://perma.cc/55GW-AAFS].

[170] *See* Taylor, *supra* note 22, at 2283–86.

[171] *See Summary of the HIPAA Privacy Rule*, *supra* note 114, at 4.

[172] *See id.*

[173] *See id.* at 9 (explaining that any authorization to disclose PHI "must be in plain language and contain specific information regarding the information to be

covered entities "make reasonable efforts to use, disclose, and request only the minimum amount of [PHI] needed to accomplish the intended purpose of the use, disclosure, or request."[174] The Privacy Rule requires all covered entities to develop written privacy policies and provide notice to individuals regarding their privacy practices.[175] Additionally, the Privacy Rule outlines a number of "Administrative Requirements."[176] For example, each covered entity must designate a "privacy official," provide privacy training to all employees, and create procedures that allow individuals to file privacy complaints.[177]

HIPAA's Security Rule applies specifically to electronic PHI ("e-PHI") and seeks to "protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care."[178] The Security Rule requires covered entities to ensure that e-PHI remains confidential and is not disclosed to any unauthorized third party.[179] Additionally, covered entities must implement safeguards against "reasonably anticipated" security threats and impermissible uses or disclosures of e-PHI.[180] Instead of mandating specific security measures, the Security Rule requires each covered entity to consider its own size, characteristics, and resources when deciding which security safeguards to implement.[181] In addition to this flexible approach, the Security Rule includes a number of administrative, physical, and technical safeguards with which all covered entities must comply.[182]

---

disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data").

[174] *Id.* at 10.

[175] *See id.* at 11, 14.

[176] *Id.* at 14–15.

[177] *See id.* at 14.

[178] *Summary of the HIPAA Security Rule*, *supra* note 114, at 2–3.

[179] *See id.* at 3.

[180] *See id.*

[181] *See id.* at 4 (noting that the Security Rule is "flexible and scalable" in recognition that "covered entities range from the smallest provider to the largest, multi-state health plan").

[182] *See id.* at 4–5.

Finally, HIPAA's Breach Notification Rule could provide further protection for femtech app users if the app experiences a data breach.[183] The Rule requires all covered entities to notify individuals following any "impermissible use or disclosure . . . that compromises the security or privacy" of PHI.[184] If any impermissible use or disclosure of PHI occurs, that event is presumed to be a breach, though this presumption is rebuttable if the covered entity can prove that PHI was likely not compromised.[185] In the case of a breach, a covered entity must provide notice to all affected individuals and the HHS Secretary; if the breach affects more than 500 individuals in a given state or jurisdiction, the media must also be notified.[186]

While amending HIPAA to include femtech apps as covered entities would massively expand the protections available for users' data, this approach poses a few considerable challenges. First, there is debate over how broadly the definition of "covered entity" should be interpreted.[187] For example, a narrow modification of the definition would cover only femtech apps that collect data using biosensors[188] (e.g., "body-invasive devices," like internal thermometers or smart tampons), while excluding apps that are merely "general health trackers."[189] This distinction, scholars argue, would balance the need to promote mobile health innovation with the need to protect users' most sensitive information.[190] However, as

---

[183] *See generally* 45 C.F.R. §§ 164.400–414.

[184] *See Breach Notification Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/8JJD-759K].

[185] *See id.*

[186] *See id.*

[187] *See* Rosas, *supra* note 3, at 323–24 (proposing a narrow redefinition of covered entities to include only the most invasive femtech apps as opposed to other scholars who suggest "a broad sweeping of mHealth applications under HIPAA's covered entity definition").

[188] *See id.* at 324 n.36 (describing biosensors as devices that convert physiological responses into data outputs).

[189] *See id.* at 323–24.

[190] *See id.* at 323–24 (arguing that redefining covered entities to include all mHealth apps would "unnecessarily burden[] all [f]emtech mobile health companies, regardless of the technology invented or the amount of personal health information collected and stored").

previously mentioned, many femtech apps collect incredibly sensitive PHI without using biosensors (e.g., through user input) and store intimate data related to menstruation, fertility, and gynecological health. Additionally, HIPAA's Security Rule lacks specificity[191] and suggests—but does not mandate—using data encryption to protect PHI.[192] The concern about encryption may be unwarranted, given that the Security Rule requires covered entities to consider factors (such as technical infrastructure, implementation costs, and any potential risks to e-PHI) when determining what security measures are "reasonable and appropriate" to implement.[193] Arguably, however, data encryption would be a reasonable and appropriate measure for femtech apps to implement, considering the intimate nature of the data collected and the risks involved with any data breaches.

V. PROPOSED ACTION: AMENDING HIPAA TO COVER FEMTECH APPS

The unregulated collection of personal, intimate data by femtech apps across the market puts millions of users' sensitive reproductive health data at risk.[194] While legal scholars have started to contemplate what actions lawmakers can take to protect femtech app users, such proposals have yet to consider solutions that provide strong data privacy protections while simultaneously exploring ways that data can contribute to women's health research. These goals need not be mutually exclusive, nor do lawmakers need to start from scratch. Amending HIPAA to cover femtech apps is the most logical avenue to improve both privacy and research outcomes. HIPAA's regulatory framework is already well-suited to ensure strong privacy and security protections for sensitive data while providing options for data to be shared with researchers. In fact, one of the main goals of HIPAA's Privacy Rule is to "strike a balance" between protecting PHI and "allowing the flow of health

---

[191] *See id.* at 337.
[192] *See id.*
[193] *See Summary of the HIPAA Security Rule*, *supra* note 114, at 4.
[194] *See* Taylor, *supra* note 22, at 2272.

information needed to . . . protect the public's health and well-being."[195]

As described above,[196] Title II of HIPPA contains rules that provide extensive protections for PHI. Certainly, the data collected by femtech apps meets HIPAA's definition of PHI.[197] Therefore, if femtech apps are considered covered entities, these HIPAA rules would ensure femtech apps (1) obtain informed authorization from users before disclosing any of their data; (2) allow app users to access their own PHI; (3) mandate security safeguards for the storage and transmission of user data that must be updated as technologies and associated risks change; and, (4) require apps to notify users if their data is used or shared in an impermissible way.

In addition to extensive privacy protections, HIPAA's Privacy Rule provides a framework for when and how PHI may be shared for research purposes.[198] Markedly, HIPAA allows covered entities to use or share PHI for research but only after obtaining an individual's written permission,[199] and it only permits unauthorized use or disclosure of PHI in a limited, specified set of circumstances; otherwise, PHI remains protected.[200] Finally, HIPAA allows for the use or dissemination of any deidentified health information for research purposes.[201] The Privacy Rule provides detailed instructions on exactly how PHI must be deidentified, including what information must be removed and how deidentification must be verified.[202] HIPAA's Privacy Rule best preserves the two competing interests at play: utilizing femtech apps' valuable health

---

[195] *See Summary of the HIPAA Privacy Rule*, *supra* note 114, at 1 (2003).

[196] *See supra*, Part IV.B.3.

[197] *See* Rosas, *supra* note 3, at 323.

[198] *See Summary of the HIPAA Privacy Rule*, *supra* note 114.

[199] *See* U.S. DEP'T HEALTH & HUM. SERVS., PROTECTING PERSONAL HEALTH INFORMATION IN RESEARCH: UNDERSTANDING THE HIPAA PRIVACY RULE 9, https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/X62Z-XP2Z].

[200] *See id.* at 9, 13 (noting that the waiver or alteration of authorization must be approved by an Institutional Review Board or Privacy Board).

[201] *See id.* at 9.

[202] *See id.* at 9–10.

data to advance women's health research and protecting users' sensitive information through privacy regulations.

Congress should amend HIPAA's definition of "covered entity" to include, at a minimum, any app that collects and stores data about users' reproductive health. Undoubtedly, amending HIPAA to include femtech apps under the definition of "covered entity" depends on congressional will. While surely a significant hurdle, HIPAA has been amended and modernized before, including for the purposes of expanding what constitutes a covered entity and adding provisions that reflect the recent shift to electronic healthcare.[203] Through such amendments, Congress and HHS have recognized HIPAA's flexibility and ensured that PHI is protected in the increasingly digital healthcare world.[204] With the recent explosion of femtech apps on the market, Congress should consider further amending HIPAA to meet the challenges of today. Congressional representatives have introduced numerous legislative proposals in recent years to address data privacy issues, including provisions for health data.[205] While there is an urgent need for broad, comprehensive data privacy legislation in the United States, Congress does not need to start from scratch when it comes to protecting data collected and stored on femtech apps. HIPAA provides an ideal regulatory framework and already protects the same types of PHI that is collected by femtech apps. Additionally, many proposed privacy laws are intended to apply broadly and

---

[203] *See* Jacqueline Bui, *Lack of Privacy Regulations in the Fitness and Health Mobile App Industry: Assessing HIPAA for Meeting the Needs of User Data Collection*, 21 UNIV. S.F. INTELL. PROP. & TECH. L.J. 1, 4–5 (2016). In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") in response to the industry-wide shift toward electronic healthcare. *See id.* at 4. Accordingly, Congress broadened the types of health plans that would be considered covered entities under HIPAA and required all "business associates" of covered entities to comply with HIPAA. *See id.* at 4–5. Then, in 2013, as a part of the Final Omnibus Rule, Congress further clarified the scope of business associates of covered entities to include downstream entities like subcontractors "even if they have an indirect relationship with a covered entity." *See id.* at 5.

[204] *See* Barbara Fox, *Mobile Medical Apps: Where Health and Internet Privacy Law Meet*, 14 HOUS. J. HEALTH L. & POL'Y 193, 214–15 (2014).

[205] *See* Keats Citron, *supra* note 4, at 1838 (identifying that "[d]ozens upon dozens of privacy bills are under consideration at the federal and state levels").

would likely not contain specific provisions that consider ways PHI can be used to advance women's health research. HIPAA, on the other hand, already contains regulations that address the concomitant privacy and research concerns around PHI and should be amended to cover the data that femtech apps collect.

VI. CONCLUSION

Every day, femtech apps collect personal, intimate data about the reproductive health of millions of users, and that number is projected to increase over the next five years. However, there are scant protections for the data these apps collect—leaving users at the whim of corporate discretion. There is an urgent need for greater privacy regulation of femtech apps to protect the sensitive and deeply personal information collected from their users. While privacy concerns are vitally important, new privacy protections must be flexible enough to allow the medical research community to utilize the valuable data collected by femtech apps to fill persistent gaps in the understanding of key women's health issues.

A privacy-protective yet malleable approach would safeguard PHI while promoting advances in public health research. As U.S. privacy law stands, the most logical and straight-forward way to accomplish these dual goals is to amend HIPAA's definition of "covered entity" to include femtech apps. If femtech apps were to constitute covered entities, Title II of HIPAA would provide an existing regulatory framework with strong privacy and security protections for the highly sensitive data collected by femtech apps. At the same time, Title II provides a pathway for the data collected by femtech apps to support critical research efforts while maintaining privacy and respecting app users' personal preferences. Amending HIPAA is not an ovary-action—by simply embracing femtech apps as covered entities under HIPAA, Congress can use the existing law to protect the millions of femtech app users whose data is currently at risk of being compromised.