Washington and Lee Journal of Civil Rights and Social Justice

Volume 30 | Issue 1 Article 7

Fall 2023

A Miscarriage of Justice: How Femtech Apps and Fog Data Evade Fourth Amendment Privacy Protections

Rachel Silver
Washington and Lee University School of Law, silver.r24@law.wlu.edu

A Miscarriage of Justice: How Femtech Apps and Fog Data Evade Fourth Amendment Privacy Protections

Rachel Silver*

Abstract

After the fall of Roe v. Wade, states across the country have enacted extreme abortion bans. Anti-abortion states, emboldened by their new, unrestricted power to regulate women's bodies, are only broadening the scope of abortion prosecutions. And modern technology provides law enforcement with unprecedented access to women's most intimate information, including, for example, their menstrual cycle, weight, body temperature, sexual activity, mood, medications, and pregnancy details. Fourth Amendment law fails to protect this sensitive information stored on femtech apps from government searches. In a largely unregulated private market, femtech apps sell health and location data to third parties like Fog Data, who in turn sell this information to police departments. According to traditional interpretations of the third-party doctrine, all reasonable expectations of privacy are eliminated when app users click "accept" to obscure privacy policies. Instead, the Supreme Court should follow the trajectory of their recent decisions and treat modern surveillance techniques differently from traditional government searches. The Court must extend Carpenter's reasoning to Fog Data because these services allow police to search billions of location data points and instantly discover personally identifying information. Congress can also strengthen privacy protections by adopting comprehensive bills that expand health privacy coverage and prevent the government from purchasing location data from private companies.

---

* J.D. Candidate, May 2024, Washington and Lee University School of Law. I would like to thank my Note Advisors, Professor Heather Kolinsky and Kaitlyn Barciszewski, for their incredible guidance and feedback throughout the Note writing process.

I. Introduction

When the New York Police Department (NYPD) found a teenage girl dead in Central Park and spotted a man fleeing the scene with her pink purse, the crime appeared to be a mugging gone wrong. The truth turned out to be more sinister and personal than anyone expected. The investigation revealed the victim was Becca, the daughter of Texas's ultra-conservative governor. According to her family, the Texas native was visiting New York for a prospective student tour and overnight program at a college. After the NYPD tracked Becca's whereabouts during the days before the incident, they discovered she skipped several college events to get coffee with an older woman. This woman admitted during police questioning that she was part of an organization that, in the wake of *Dobbs v. Jackson Women's Health*,[1] helps women travel across states to obtain legal abortions. Becca orchestrated the college visit as a cover story to get permission from her conservative, pro-life parents to visit New York. The real reason she came to New York was to get a legal abortion because her home state of Texas had recently banned abortions from the moment of fertilization.

In the end, her family, who claimed to be avid pro–life advocates, killed Becca for defying their beliefs and getting an abortion. Her own mother encouraged Becca's brother to follow Becca to New York and confront her about the pregnancy. In a text message that the NYPD uncovered, the brother lashed out with

1. 142 S.Ct. 2228 (2022).

death threats before leaving Texas, telling his mother he wanted to "f***ing kill [Becca]" for seeking an abortion. Most damning, the woman who helped Becca get the abortion witnessed Becca's brother murder Becca.

But how did Becca's family even know she was pregnant? Becca's mother, without her consent or knowledge, had hacked into her period tracking app.

Becca's story did not actually happen. Her tragedy is the plot of the Law & Order episode "Battle Lines."[2] Nevertheless, what happened to Becca represents the very real consequences of criminalizing women's health care. While Becca's story was dramatized for TV, it reflects the haunting realities of a post-*Roe* world.[3] After the Supreme Court removed any constitutional protection for abortions, many states have banned or severely restricted abortion, stripping away women's reproductive autonomy and opening the door to dangerous invasions of privacy rights.

In June 2022, the landmark *Dobbs v. Jackson Women's Health Organization* decision held that the United States Constitution does not confer a right to abortion.[4] The Supreme Court overruled both *Roe v. Wade*[5] and *Planned Parenthood v. Casey*[6], giving individual states the full power to regulate any aspect of abortion.[7] In response, eleven states have already enforced bans that prohibit

2. *See Law & Order: Battle Lines* (NBC television broadcast Sept. 29, 2022) (depicting the murder investigation of a teenage girl who sought abortion care in New York).

3. *See* Marin Cogan, *What "Choice" Means for Millions of Women Post-Roe*, VOX (Jan. 20, 2023, 6:00 AM) ("A 10-year-old victim of rape was forced to cross state lines to receive an abortion. Women were denied care while having miscarriages due in part to confusion among health providers. Thirteen states enacted trigger laws, which banned nearly all abortions . . . while other states moved to severely restrict the procedure.") [perma.cc/4MZT-G3Q2].

4. *See* Dobbs v. Jackson Women's Health Org., 142 S.Ct. 2228, 2242 (2022) ("We hold that *Roe* and *Casey* must be overruled. The Constitution makes no reference to abortion, and no such right is implicitly protected by any constitutional provision, including the one on which the defenders of *Roe* and *Casey* now chiefly rely—the Due Process Clause of the Fourteenth Amendment.").

5. 410 U.S. 113 (1973).

6. 505 U.S. 833 (1992).

7. *See Dobbs*, 142 S.Ct. at 2242–43 ("It is time to heed the Constitution and return the issue of abortion to the people's elected representatives.").

abortion entirely.[8] Most laws criminalizing abortion only aim to punish the provider and those who assist with obtaining abortion services.[9] Some state laws are clear that doctors, nurses, clinic staff, abortion fund staff and volunteers, as well as friends and family who help patients in obtaining an abortion, will face legal consequences.[10] Still, some abortion bans are unclear as to whom the law seeks to punish, and multiple states are already criminalizing the women who receive abortions.[11]

It is estimated that, even before *Dobbs,* more than 1,200 women were arrested across the United States based on their pregnancy outcomes.[12] Most of these women were "charged with felonies like concealment of a birth, practicing pharmacy without a license, or even homicide."[13] And at least 38 states have laws that make it a crime to harm a fetus and three states explicitly criminalize self-managed abortion.[14] In practice, fetal harm laws have been "used to investigate and prosecute a variety of pregnancy loss, including miscarriages, stillbirths, and self-

8. *See Abortion Is Now Illegal in 11 U.S. States*, CTR. FOR REPROD. RTS. (Aug. 30, 2022) (tracking state bans in Alabama, Arkansas, Idaho, Kentucky, Louisiana, Mississippi, Missouri, Oklahoma, South Dakota, Tennessee, and Texas that have already left millions without abortion care) [perma.cc/GV7L-D9LJ].

9. *See* Elyssa Spitzer, *Some States are Ready to Punish Abortion in a Post-Roe World,* CTR. FOR AM. PROGRESS (June 4, 2022) (providing summaries of each state's abortion ban) [perma.cc/XAT7-RV5FD].

10. *See* Aliyah Tihani Salim & Shivana Jorawar, *Roe Is Over. Prison Sentences Are on the Way.*, NBC NEWS: THINK (July 3, 2022, 5:40 AM) (recognizing the changing legal landscape after *Dobbs* and predicting more criminal punishment for family planning decisions) [perma.cc/GHJ2-2QY3].

11. *See* Aaron Blake, *The GOP and Where it's Headed on Criminalizing Abortion*, WASH. POST (May 11, 2022, 5:07PM) (describing how states have responded to the Supreme Court's decision to overturn *Roe,* including the complete criminalization of abortion care) [perma.cc/Z9Q3-9VSJ].

12. *See* Farah Diaz-Tello, *Roe Remains for Now . . . Will It Be Enough?*, 45 HUM. RTS. MAG. 14, 16 (Aug. 2020) ("There have been more than 1,200 women arrested across the United States based on their pregnancy outcomes—including miscarriages, stillbirths, abortions, or neonatal losses—since Roe was decided").

13. *Id.*

14. *See* Robert Baldwin, *Losing a Pregnancy Could Land You in Jail in Post-Roe America*, NPR (July 3, 2022) (outlining the history of prosecuting pregnancy loss under fetal harm and murder statutes) [perma.cc/JYR2-CZTJ].

induced abortions."[15] In 2015, Purvi Patel was prosecuted under Indiana's feticide law for taking safe, effective and commonly used abortion medications.[16] Patel was sentenced to 20 years in prison, but her conviction was overturned after serving 18 months.[17] And in Tennessee, Anna Yocca, was charged with attempted murder for trying to use a coat hanger to end her pregnancy.[18] Yocca spent over a year behind bars before pleading to a lesser charge—"attempted procurement of a miscarriage"—in exchange for her release.[19]

Following the *Dobbs* decision, more women are being prosecuted for seeking or assisting others with abortions. In February 2023, a woman in South Carolina was arrested and awaits trial for using abortion pills to end her pregnancy.[20] In July 2023, an 18-year-old Celeste Burgess from Nebraska was sentenced to 90 days in jail and two years of probation after pleading guilty to "illegally concealing human remains."[21] Celeste and her mother, Jessica Burgess, were charged in 2022 after the police obtained their private Facebook messages discussing their

15. *Id.*; *see also* Shaila Dewan & Sheera Frenkel, *A Mother, a Daughter and an Unusual Abortion Prosecution in Nebraska*, N.Y. TIMES (Aug. 18, 2022) (showing how prosecutors have made "creative use" of laws not related to abortion to criminalize miscarriages and abortions that occur outside of clinical settings) [perma.cc/7K2Y-BUU9].

16. *See* Salim, *supra* note 10 (highlighting stories of women who were criminally charged for self–induced abortions).

17. *Id.*

18. *Id.*

19. *See* Daniella Silva, *Anna Yocca, Tennessee Woman in Coat-Hanger Attempted Abortion Case, Released from Jail a Year Later*, NBC NEWS (Jan. 11, 2017, 9:09 AM) ("Anna Yocca, 32, pleaded guilty to 'attempted procurement of a miscarriage' on Monday after spending one year and one month in prison while awaiting trial in a case where she was originally charged with attempted murder . . . .") [perma.cc/7X7R-HDYH].

20. *See* Poppy Noor, *South Carolina Woman Arrested for Allegedly Using Pills to End Pregnancy*, GUARDIAN (Mar. 3, 2023, 3:32 PM) ("The incident took place in 2021, before the constitutional right to abortion was overturned in June 2022. But a warrant was subsequently issued for the woman's arrest in 2022, and she was arrested in February 2023 . . . .") [perma.cc/X4QJ-72H7].

21. Michael Levenson, *Nebraska Teen Who Used Pills to End Pregnancy Gets 90 Days in Jail,* N.Y. TIMES (July 20, 2023) [perma.cc/N72H-LMP7].

plans to end the pregnancy with abortion pills.[22] The mother also pled guilty in July to violating Nebraska's abortion law and "removing or concealing human remains,"[23] and she was sentenced to two years in prison.[24] Elizabeth Ling, from the If/When/How abortion rights group, stated, "I am disturbed and appalled that, despite self-managed abortion not being illegal in Nebraska, prosecutors chose to punish a young person by wrongfully weaponizing their laws against them for allegedly ending their own pregnancy."[25] Meanwhile, in Texas, a man is suing three women under a wrongful death statute, "alleging that they assisted his ex-wife in terminating her pregnancy."[26] His lawsuit claims that assisting an abortion qualifies as murder under state law, which would allow him to sue under this civil statute.[27] States continue to criminalize women, and those assisting them, for receiving abortion care, and prosecutors use a variety of criminal statues to charge them.

In January 2023, Steve Marshall, Alabama's attorney general and a staunch opponent of abortion rights, issued a statement that pregnant women could be prosecuted for taking abortion pills.[28] Marshall emphasized that Alabama's ban "targeting abortion providers does not preclude the state from seeking to penalize

22. *See id.* (noting that the mother and daughter were charged after "police obtained their private Facebook messages, which showed them discussing plans to end the pregnancy and 'burn the evidence.'").

23. *Id.*

24. *Id.*; *see also* Mitchell McCluskey, *A Nebraska Mother Who Provided an Illegal Abortion for her Daughter and Helped Dispose of the Fetus Gets 2 Years in Prison, Report Says*, CNN (Sept. 22, 2023, 9:30 AM) (providing an update that Jessica Burgess was sentenced to two years in prison) [perma.cc/243G-AT2F].

25. Levenson, *supra* note 21.

26. *See* Eleanor Klibanoff, *Three Texas Women are Sued for Wrongful Death after Allegedly Helping Friend Obtain Abortion Medication,* TEX. TRIB. (Mar. 10, 2023, 4:00 PM) (reporting on the first wrongful death lawsuit of its kind since the *Dobbs* decision) [perma.cc/8HXQ-A3ZK].

27. *See id.* (discussing the views of legal experts who see this case as potentially setting a dangerous precedent in future criminal proceedings).

28. *See* Caroline Kitchener & Ellen Francis, *Talk of Prosecuting Women for Abortion Pills Roils Antiabortion Movement,* WASH. POST (Jan. 11, 2023, 9:34 PM) ("Alabama's attorney general became the most prominent Republican official yet to suggest that pregnant women could be prosecuted for taking abortion pills . . . .") [perma.cc/V77G-GB7N].

women under other existing laws."[29] He suggested pregnant women could be prosecuted under a separate chemical endangerment law which punishes women for drug consumption during pregnancy.[30] In September 2022, Marshall also confirmed he would prosecute who people help Alabama women obtain out-of-state abortions.[31] He explained, "If someone was promoting themselves out as a funder of abortions out of state, that is potentially criminally actionable for us. If there are groups promoting this as part of their services, we will be taking a look at that."[32] Individuals and groups supporting out of state abortions could face felony charges in Alabama for accessory and conspiracy crimes.

Multiple state legislators have also presented bills that would broaden abortion bans to include women seeking abortions. Oklahoma lawmakers presented a bill that eliminates provisions in their abortion law which previously protected pregnant women from criminalization.[33] And bills recently introduced in Texas, Kentucky, and South Carolina aim to establish that life begins at conception, granting personhood to fetuses.[34] These personhood bills explicitly subject women seeking abortion to homicide charges.[35] And homicide is still punishable by death in those

29. *Id.*

30. *See id.* (quoting Marshall's statement that Alabama's abortion ban "does not provide an across-the-board exemption from all criminal laws, including the chemical-endangerment law – which the Alabama Supreme Court has affirmed and reaffirmed protects unborn children").

31. *See* Josh Moon, *Alabama AG: State May Prosecute Those Who Assist in Out-of-State Abortions,* ALA. POLI. REP. (Sept. 22, 2022, 6:30 AM) ("In Alabama, the volunteers who help women [seek out-of-state abortions] could face jail time due to the state's 'accessory provisions' and 'conspiracy provisions,' according to Alabama Attorney General Steve Marshall.") [perma.cc/3JXE-4SFX].

32. *Id.*

33. *See* Shefali Luthra, *Abortion Bans Don't Prosecute Pregnant People. That May Be About to Change.*, 19TH NEWS (Jan. 13, 2023, 1:05 PM) (warning about new state legislative efforts to punish people who induce their own abortions) [perma.cc/8EUJ-8HCK].

34. *See* Poppy Noor, *Republicans Push Wave of Bills That Would Bring Homicide Charges for Abortion*, GUARDIAN (Mar. 10, 2023, 6:00 AM) ("The bills being introduced in Arkansas, Texas, Kentucky and South Carolina look to establish that life begins at conception. Each of these bills explicitly references homicide charges for abortion.") [perma.cc/UDG4-PRX8].

35. *See* H.R. 1174, 94th Gen. Assemb., Reg. Sess. (Ark. 2023) ("To ensure the right to life and equal protection of the laws, all unborn children should be

states.[36] This recent wave of bills "exposes *a fundamental lie* of the anti-abortion movement, that they oppose the criminalization of the pregnant person."[37] These laws explicitly target women seeking abortions, not just their medical providers or supporters, and some bills even place women in jeopardy of receiving the death penalty for their healthcare decisions. Despite their ostensible "pro-life" slogan, the anti-abortion movement does not prioritize women's safety or freedom and anti-abortion lawmakers have only become more emboldened after *Dobbs*.

Within this hostile climate, privacy concerns over reproductive health information stored in women's phones, particularly in period tracking apps, have grown—and rightly so.[38] Depending on the app, companies can store and share information on users' "weight, temperatures, moods, reading material, sexual encounters, tampon use, alcohol consumption, cigarette and coffee

protected under the state homicide laws as all other persons."); H.R. 300, 2023 Gen. Assemb., Reg. Sess. (Ky. 2023) ("[T]o ensure the right to life and equal protection of the laws, all preborn children should be protected with the same homicide laws protecting all other human persons."); H.R. 3549, 125th Gen. Assemb., Reg. Sess. (S.C. 2023) ("In a prosecution under this article where the victim is an unborn child, unless specifically provided otherwise: enforcement is subject to the same presumptions, defenses, justifications, laws of parties, immunities, and clemencies as would apply to the homicide of a person who had been born alive.").

36. *See* Noor, *supra* note 34 ("Each of these bill explicitly references homicide charges for abortion. Homicide is punishable by the death penalty in all of those states.").

37. *Id.*

38. *See* Madison Harris, *The New Dangers Surrounding Period-Tracking Apps*, IN OUR OWN VOICE: NAT'L BLACK WOMEN'S REPROD. JUST. AGENDA (Aug. 31 2022) ("After the overturning of *Roe v. Wade*, there is a growing possibility that data from period-tracking apps could be obtained as evidence to support a criminal loss of pregnancy, even in instances of miscarriage.") [perma.cc/BE2T-BK57]; Jasmine Wright & Maegan Vazquez, *White House Says Americans Should Be 'Really Careful' About Using Period Tracker Apps*, CNN (July 8, 2022, 3:19 PM) ("The White House is warning individuals to be 'really careful' when using phone apps that track users' menstrual cycles over fears that the data could be used against them if they seek abortions following the Supreme Court's decision to overturn *Roe v. Wade*.") [perma.cc/9NF5-CNCL]; Tatum Hunter & Heather Kelly, *With Roe Overturned, Period-Tracking Apps Raise New Worries*, WASH. POST (June 24, 2022, 2:30 PM) ("With 13 states poised to ban abortion after a Friday Supreme Court decision overturning the right to get one, many worry that data from period apps could become evidence of a crime.") [perma.cc/6LCV-W9HB].

habits, bodily secretions, and birth control pills."[39] In states where abortion is now illegal, women may worry that the government will use the sensitive health information in their period tracking app to discover they had an abortion and then prosecute them, their family, or healthcare provider.

In a hypothetical situation where the government tracks a woman seeking an abortion, a future criminal investigation may involve multiple steps. First, the police could use location tracking technology to determine who is traveling to a women's health clinic to potentially receive abortion care. Then, after identifying suspects, the police may also get a court order for the health information stored on a period or fertility app to determine whether the suspect had lost a pregnancy.

Part II of this Note examines the type of information that period and fertility tracking apps collect and sell to third parties. Then, Part III will provide an overview of relevant Fourth Amendment jurisprudence, including the third-party exception to Fourth Amendment protections and the Supreme Court's approach to advanced, evolving location tracking technologies. Part IV argues that the Fourth Amendment fails to provide sufficient privacy protections for both (1) the extremely personal health data stored on period and fertility apps and (2) the massive amount of location data that third party companies such as Fog Data gather and sell to law enforcement. Part V encourages courts to re-examine the third party doctrine and to extend the principles from *Carpenter* to Fog Data's subscription services. The third–party doctrine should not apply when the government pays to peer through an "intimate window" into lives of millions of unsuspecting citizens. Alternatively, Part VI proposes that the legislature can enact laws, such as the proposed Protecting Personal Health Data Act and the Fourth Amendment Is Not for Sale Act, to strengthen privacy protections for sensitive health and location data.

39. Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1775 (2021).

II. Fertility and Period Tracking Apps Jeopardize Individual Privacy Rights When They Collect and Share Extremely Personal Information

In the landmark case *Riley v. California,* the Supreme Court recognized how the immense storage capacity of cellphones distinguishes them from other physical records the government may search.[40] Chief Justice Roberts emphasized that:

> Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; *apps for tracking pregnancy symptoms*; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely (emphasis added).[41]

As the Chief Justice recognized, cellphone apps store an unprecedented amount of information about a person's everyday life. Previously, when a government searched a person's pockets or even their home filing cabinets, this search would be limited in scope, detail, and time.[42] Now, modern cellphone technology allows the government to scour through an unlimited database of highly sensitive information.[43] Unlike traditional paper calendars women used to rely on to track their menstrual cycles, femtech apps gather

---

40. *See* Riley v. California, 573 U.S. 373, 393, 403 (2014) ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.").

41. *Id.* at 396.

42. *See id.* at 393–96 (distinguishing government searches of cellphones from searches of other physical records and personal items).

43. *See id.* at 393 ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as telephones. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

and record personal information that extends far beyond the date of a woman's last period.[44]

"Femtech" apps are a popular collection of women's health apps that collect extremely personal, detailed, and extensive data about users' everyday life and well-being.[45] The term "femtech" describes "apps, services, products, and sites that collect information about women's period cycles, fertility, pregnancies, menopause, and sexual and reproductive histories."[46] There are four popular femtech apps: Flo, MyCalendar, Baby Center, and Glow.[47] Each app gathers personal health information from data users manually enter and data the apps gather passively in the background.[48] Then, the femtech apps share consumers' information with law enforcement and various third parties for advertising or other business purposes, and the femtech companies may or may not disclose which entities they sell data to.[49]

---

44. *See infra* Subparts 0.A., II.B. (describing the personal health and location data that femtech apps collect).

45. *See* Citron, *supra* note 39, at 1774–77 ("Nearly one-third of women in the United States have used period-tracking apps. Menstrual tracking apps 'are the fourth most popular health app among adults and the second most popular among adolescent females.'") (citing Michelle L. Moglia et al., *Evaluation of Smartphone Menstrual Cycle Tracking Applications Using an Adapted APPLICATIONS Scoring System*, 127 OBSTETRICS & GYNECOLOGY 1153, 1153 (2016)); *see also* Jerry Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Report Finds,* CONSUMER REPS. (Sept. 17, 2020) ("Glow also asks for intimate physical details, including the appearance of their cervical mucous and the position of their cervix (the app has instructions for determining these characteristics), any history of abortions, whether they've experienced anything from diarrhea to low sex drive, their mood, and more.") [perma.cc/B5S2-EBZK].

46. Citron, *supra* note 39, at 1774–75.

47. *See* Donna Rosato, *What Your Period Tracker App Knows About You,* CONSUMER REPS. (Jan. 28, 2020) (comparing five popular femtech apps' privacy policies "for clarity and comprehensiveness, transparency about data sharing, user control over their information and access to it") [perma.cc/5L76-KWKW].

48. *See infra* Subparts 0.A., II.B. (listing the substantial amount of personal data femtech apps gather with and without user's affirmative consent or acknowledgement).

49. *See infra* Subpart II.B. (highlighting how femtech apps comply with law enforcement and sell data to third parties).

A. Users Manually Enter Personal Information into Femtech Apps

The first type of information femtech apps collect and store is subscriber information. When users sign up and make an account with a period or fertility tracking app, the app begins to gather personally identifying information, such as their login information, contact details, and demographic backgrounds.[50] The femtech apps may store a user's name, email address, passwords, phone numbers, postal address, nationality, gender, age, and more.[51]

Of course, subscribers then enter various details related to their personal health and wellbeing to utilize the main features of these apps—menstrual cycle and fertility tracking. But the health data collected in these apps goes far beyond recording menstrual cycle dates and fertility status. Across all the major apps, users enter sensitive health information.[52] Flo and Glow also allow users to connect with other health apps like Apple HealthKit, Samsung Health, Google Fit, or MyFitnessApp.[53] If users give permission to

---

50. *See, e.g.*, *Glow Privacy Policy*, GLOW (Oct. 25, 2022) ("Personal information [users] may provide to us through the Service or otherwise includes: account data that [they] provide to create an account on the Service, including [their] name, email address, password, date of birth and mobile phone number.") [perma.cc/S564-54MK].

51. *See Privacy Policy,* FLO (Sept. 14, 2022) [hereinafter *Flo Privacy Policy*] ("When you sign up to use the Services, we may collect Personal Data about you such as: name; email address, year of birth; password or passcode; place of residence and associated location information including time zone and language; ID (for limited purposes).") [perma.cc/PCY2-MZCG]; *Glow Privacy Policy*, *supra* note 50 (detailing the account data and profile data the app collects); *BabyCenter Privacy Policy*, BABYCENTER (February 1, 2023) (describing the personal details, demographic information, and contact details that BabyCenter collects from users) [perma.cc/RPT4-FLSF].

52. *See My Calendar – Period Tracker Privacy Policy,* SIMPLEINNOVATION (Aug. 31, 2023) [hereinafter *My Calendar Privacy Policy*] (listing data collected, including name, email address, menstrual cycle and period dates and length, symptoms and moods, sexual activity, contraceptive methods, medicines, temperature, and weight) [perma.cc/PPG8-ZXWZ]; *Glow Privacy Policy*, *supra* note 50 ("Personal information we collect . . . health data such as information about your physical attributes, sexual orientation, fertility, pregnancy, sexual activity, menstrual activity, sleep activity, mood, health conditions, medications, and number of children."); *BabyCenter Privacy Policy*, *supra* note 51 (listing the categories of personal information that BabyCenter stores).

53. *See Glow Privacy Policy, supra* note 50 (explaining how users can share health data from mobile health apps, such as Apple HealthKit, Samsung Health,

import data from other health apps, Glow and Flo gain access to additional information such as sports activities, calories burned, heart rate, and number of steps/distance traveled.[54] Overall, the femtech apps are more than an electronic calendar; they collect extensive data on users' health and wellbeing that can create a comprehensive picture of an individual's private life.

Moreover, Glow and Baby Center make public spaces available for users to share their health status with others. For example, Glow has discussion boards where users talk to each other about "their intimate lives, including their experiences with sex, fertility, abortions, or miscarriages."[55] Glow tracks and stores all these communications.[56] Similarly, Baby Center encourages women to share photos of their bellies on public community forums to visually track their pregnancies.[57] Glow and BabyCenter also track browsing history on their platforms (if someone searched for discussions on abortions).[58] On public discussion boards and forums, users broadcast extremely intimate health data with the femtech apps and with the app's millions of subscribers.

B. Femtech Apps Automatically Collect Information About Users

Along with information that users knowingly give to femtech apps, the apps automatically gather other data behind the scenes

---

Google Fit, and MyFitnessApp, with Glow); *Flo Privacy Policy, supra* note 51 ("[Users] may also allow us to connect to third-party services, such as Apple HealthKit and Google Fit, to enable us to import Personal Data about your health and activities into the App.").

54. *Flo Privacy Policy*, *supra* note 51; *Glow Privacy Policy*, *supra* note 50.

55. Citron, *supra* note 39, at 1776.

56. *See id.* (describing users' approaches to the discussion boards, such as losing their "inhibition because so many other women are talking about their intimate lives on the discussion boards") (internal quotations omitted).

57. *See* Rosato, *supra* note 47 ("[BabyCenter] requests access to a user's camera—something the other apps CR looked at don't do—so pregnant users can take photos of their bellies. Those photos can be stored in the user's device and in the cloud . . . .").

58. *See Glow Privacy Policy*, *supra* note 50 (mentioning that Glow collects data on online browsing between different pages and services); *BabyCenter Privacy Policy*, *supra* note 51 (stating BabyCenter records browsing history and searches on the platform).

as users interact with the app. The femtech apps automatically collect information on user's device model and settings, IP address, mobile service provider, and advertising IDs.[59]

Location tracking data and advertising IDs are the most relevant to this Note and will be discussed in later sections.[60] Femtech apps gather location information from users, with and without their affirmative permission.[61] All the apps automatically gain "non-precise" location information (at the city or zip code level) on a user's device based on such device's IP address.[62] Even more concerning, some apps, like Glow, gather precise geographical location data when users authorize the app to access their device's location.[63]

An advertising ID is a device identifier that third party companies use for online behavioral advertising.[64] Depending on whether an individual has an iOS or Android device, Apple or Google creates and manages an advertising ID associated with their mobile device.[65] Femtech apps sell advertising IDs to

---

59. *See My Calendar Privacy Policy*, *supra* note 52 (explaining the types of analytics data, advertising data, and purchase data that My Calendar collects.); *Flo Privacy Policy*, *supra* note 51 (listing automatically collected information, including device information and location information); *Glow Privacy Policy*, *supra* note 50 (detailing passively collected information including devices data, online activity data, and precise geolocation data).

60. *See infra* Part IV.B. (arguing data brokers and private companies like Fog Data contravene core Fourth Amendment principles).

61. *See, e.g.*, *Glow Privacy Policy*, *supra* note 50 (offering the ability to opt-out on the "collection of "precise geolocation data when you authorize our mobile application to access your device's location.").

62. *See Flo Privacy Policy*, *supra* note 51 (listing automatic information Flo gathers including IP addresses); *Glow Privacy Policy*, *supra* note 50 (identifying device data that Glow collects including IP addresses); *My Calendar Privacy Policy*, *supra* note 52 (stating information collected may include "a device identifier enabling other issues on the same device to be located"); *BabyCenter Privacy Policy*, *supra* note 51 (mentioning, in the middle of many obscure technical terms, that BabyCenter processes IP addresses).

63. *See Glow Privacy Policy*, *supra* note 50 ("[Users] can use [their] mobile device's privacy settings to disable our access to any data granted through them, such as [their] device's precise geolocation . . . .").

64. *See My Calendar Privacy Policy, supra* note 52 ("Advertising IDs are standard across the mobile advertising industry and are used to identify a particular device for advertising purposes. Advertising IDs are random identifiers that are generated by and tied to your mobile device.").

65. *See* Bennett Cyphers, *How to Disable Ad ID Tracking on iOS and Android, and Why You Should Do It Now*, ELEC. FRONTIER FOUND. (May 11, 2022)

advertisers who collect information, under the specific advertising ID, about a user's online activities over time and across different websites and apps.[66] Then, the advertisers provide interest-based advertising or other targeted content to the individual's mobile device.[67]

But the Electronic Frontier Foundation (EFF)[68] warns that this unique string of letters and numbers in an advertising ID does not merely provide tailored advertising; advertising IDs exist for "one purpose: to help companies track you."[69] Although companies may claim advertising IDs do not contain "personally identifying" information, this is simply not true in practice.[70] Advertising IDs are often used to collect personally identifiable data like specific location data.[71] As the EFF notes, "if you can see where a person works, sleeps, studies, socializes, worships, and seeks medical care," further information, such as a person's email address or phone number, is not needed to identify them.[72] While advertising IDs may appear harmless to the average femtech app user, they are "ubiquitous and effective" identifiers in the tracking industry.[73]

("The ad identifier . . . is the key that enables most third-party tracking on mobile devices. Disabling it will make it substantially harder for advertisers and data brokers to track and profile you, and will limit the amount of your personal information up for sale.") [perma.cc/4JRE-92G6].

66. *See Case Study Reproductive Health Apps*, DIGIT. STANDARD (Jan. 2020) (evaluating the security and privacy of popular femtech apps) [perma.cc/S6RS-D2P3].

67. *See My Calendar Privacy Policy*, *supra* note 52 (describing how advertisers collect information using advertising IDs to generate tailored content for users).

68. *About EFF*, ELEC. FRONTIER FOUND. (explaining that EFF is a leading nonprofit organization that "champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development") [perma.cc/U4ZK-M8FA].

69. *See* Cyphers, *supra* note 65 (summarizing how different companies can link and compare datasets about a user to create a profile with a wide range of information).

70. *See id.* ("[A]n entire industry exists to help trackers link ad IDs to more directly identifying information, like email addresses and phone numbers.").

71. *See id.* ("[T]he ad ID is commonly used to help collect data that is obviously personally identifiable, like granular location data.").

72. *Id.*

73. *See id.* (warning readers about the dangers of the advertising ID tracking industry).

C. Femtech Apps Breach Users' Privacy When They Share Data with Law Enforcement and Third–Party Companies

Each major femtech app admits that their company will comply with law enforcement requests and may hand over personal data for criminal investigations.[74] For example, Glow's privacy policy states, "We may use your personal information to: comply with applicable laws, lawful requests, and legal process, such as to respond to subpoenas or requests from government authorities."[75] If law enforcement suspects an individual committed an illegal abortion, they could simply request that a femtech app disclose all personal information gathered on the individual and use their health data to confirm whether they lost a pregnancy.

All the major femtech apps also share and sell their user data with external partners for other purposes such as targeted advertising.[76] Comparing the four femtech apps, Glow and BabyCenter provide the least privacy protection or transparency for users while My Calendar and Flo have attempted to limit what data is shared with third parties and disclose who they are partnering with.

Glow and BabyCenter pose more danger to users' privacy because the apps may share personal health data with third parties and do not disclose which third parties they work with.[77] Glow may share "personal data" with unnamed third parties for marketing and advertising, and this personal data encompasses

---

74. *See My Calendar Privacy Policy, supra* note 52 ("[W]e may also use your Personal Information to respond to a valid and enforceable court order, law, or legal process."); *Flo Privacy Policy, supra* note 51 (allowing the company to share personal data "in response to subpoenas, court orders or legal processes, to the extent permitted and as restricted by law"); *BabyCenter Privacy Policy*, *supra* note 51 ("We may disclose your User Information to legal and regulatory authorities (including law enforcement agencies and courts) to respond to legal requests or orders, comply with applicable law, or exercise or defend our legal rights.").

75. *Glow Privacy Policy, supra* note 50.

76. *See* Rosato, *supra* note 47 (providing a table indicating that BabyCenter, Clue, Flo, My Calendar, and Ovia share data with third parties, including advertisers and marketers).

77. *See Glow Privacy Policy*, *supra* note 77 (failing to specify the third parties involved); *BabyCenter Privacy Policy*, *supra* note 51 (same).

intimate health data, account data, and automatic technical data (IP address, advertising IDs, etc.).[78] Glow's privacy policy says users have to affirmatively opt out of "Key Health Data" to remove their period data and health logs from the app's servers and to protect it from being shared with others.[79] BabyCenter also shares user information without permission. The Company shares, to undisclosed third parties, a variety of personal and technical information, including "information provided in response to quizzes or surveys or to use certain health-related programs, such as weight goals and caloric intake, and photographs."[80] While BabyCenter's 8,500-word privacy policy states that they do not process "sensitive data," the Company does not define what this includes and shares user data nonetheless.[81] Glow and BabyCenter both share intimate personal data with an unknown amount of third parties.

In contrast, My Calendar only shares technical information with third parties and discloses which companies it partners with for advertising purposes. My Calendar's privacy policy lists eight companies it shares information with, including Google, Amazon, and Facebook.[82] These third parties "may use and disclose aggregated, or otherwise anonymized information that does not relate to an identifiable natural person without restriction."[83] Although My Calendar claims to only provide "anonymous" data to third parties, it does share advertising IDs with companies, which can be used to track and locate individuals.[84]

---

78. *See Glow Privacy Policy, supra* note 50 (listing the types of information Glow sells to advertisers); *BabyCenter Privacy Policy, supra* note 51 (same).

79. *See Glow Privacy Policy, supra* note 50 (mentioning affirmation steps users can take to restrict the sale of their data).

80. *BabyCenter Privacy Policy, supra* note 51.

81. *See id.* (concealing the meaning of their privacy policies in lengthy, technical language).

82. *See My Calendar Privacy Policy*, *supra* note 52 (providing a chart with detailed information about with whom My Calendar shares data).

83. *Period Calendar, Cycle Tracker*, MY CALENDAR PERIOD TRACKER (Dec. 6, 2019) [perma.cc/72SW-7HFQ].

84. *See id.* (failing to recognize that advertising IDs are used to trace the whereabouts of individuals).

Similar to Glow and BabyCenter, Flo used to share personal health data with social media giants like Facebook.[85] Yet in 2019, Flow stopped using Facebook as an advertising partner after the Wall Street Journal revealed that Flo told the social media company when a user was having her period or intending to get pregnant.[86] Now, Flo uses only one partner for ad targeting. Flo may provide "non-health personal data" with its partner AppsFlyer for marketing and promotional purposes.[87] For Flo, "non-health personal data" includes technical identifiers like IP addresses and advertising IDs, an individual's age group, their subscription status, and "the fact of an application launch."[88] While Flo's change in policy offers more privacy for highly personal health data, the technical identifiers sold to third parties are still a problematic source of location tracking.

Disclosure of third-party transactions is only a first step in protecting individual privacy because selling technical identifiers, like advertising IDs, lead to invasive location tracking tactics. Fog Data Science ("Fog Data") is a private company that demonstrates the dangers of femtech apps selling advertising IDs to third parties. Fog Data is a Virginia-based company that captures and stores "billions of location data points taken from millions of people's cell phones."[89] Fog Data purchases geolocation data originally collected by thousands of smartphone apps—including femtech apps. As described above, apps constantly gather location data about where a phone is using unique advertising IDs and then

85. *See* Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook,* WALL ST. J. (Feb. 22, 2019: 11:07 AM) ("Flo Health Inc.'s Flo Period & Ovulation Tracker, which claims 25 million active users, told Facebook when a user was having her period or informed the app of an intention to get pregnant, the tests showed.") [perma.cc/4XGN-MUXD].

86. *Id.*; *see also* Rosato, *supra* note 47 ("[T]he Wall Street Journal revealed last February that [Flo] shared personal data, such as whether a user intended to become pregnant, with the social media giant, which used the information for targeted advertising.").

87. *See Flo Privacy Policy, supra* note 51 (stating that Flo only shares users' non-health information with the third party AppsFlyer and providing a graphic to illustrate how AppsFlyer processes this information from Flo).

88. *Id.*

89. Bennett Cyphers & Aaron Mackey, *Fog Data Science Puts Our Fourth Amendment Rights Up for Sale,* ELEC. FRONTIER FOUND. (Aug. 31, 2022) [perma.cc/HZ6W-V5XN].

sell it to data brokers.[90] Fog Data buys this information from data brokers and, in turn, offers a "massive, searchable database" to law enforcement for a subscription fee.[91] Local police departments pay Fog Data to see where a person has been at any given moment over the past several years.[92]

EFF expert, Bennett Cyphers, warned, "This data could be used to search for and identify everyone who visited a Planned Parenthood on a specific day . . . The potential for abuse is staggering, and from what we've found so far, there are few or no rules protecting our constitutional rights."[93] Without effective legal protections, the police in states criminalizing abortions could use Fog Data services to identify and track women who receive abortion care at women's health clinics.

III. The Fourth Amendment Is Supposed to Prevent the Government from Intruding Upon a Reasonable Expectation of Privacy

To determine whether the Fourth Amendment protections apply to the vast, detailed personal information collected on femtech apps, this Section will provide an overview of Fourth Amendment jurisprudence, highlighting key cases about the third-party doctrine and location tracking technology.

---

90. *See* Matthew Guariglia, *What is Fog Data Science? Why is the Surveillance Company so Dangerous?*, ELEC. FRONTIER FOUND. (Aug. 31, 2022) (explaining that Fog Data "purchases raw geolocation data originally collected by applications" which "gather location data about where your phone is at any given moment and sell it to data brokers, who in turn sell it most often to advertisers or marketers who try to serve you ads based on your location") [perma.cc/L5V9-4EHL].

91. *See id.* (describing how law enforcement can use the location data, including identifying devices within a specified area and tracing a device's location history).

92. *See id.* (same).

93. *Data Broker Helps Police See Everywhere You've Been with the Click of a Mouse: EFF Investigation,* ELEC. FRONTIER FOUND. (Sept. 1, 2022) [perma.cc/GJ9T-AA76].

A. Traditionally, Fourth Amendment Privacy Protections Apply Only If the Government Either (1) Trespasses onto to Physical Property or (2) Invades a Reasonable Expectation of Privacy

The Fourth Amendment grants people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[94] The Fourth Amendment emerged in response to the unfettered power of British authorities during colonial America.[95] Under the law of general warrants, British officers could rummage through homes at any time for any reason and collect evidence of criminal activity.[96] Thus, the Founders introduced the Fourth Amendment to protect individuals against arbitrary government interference and surveillance.[97] Today, the government must secure a warrant supported by probable cause for most search and seizure activities.[98] If authorities conduct an unreasonable search or seizure without a proper warrant, the evidence obtained will be excluded during a criminal trial.[99]

For Fourth Amendment protections to apply, the government must conduct a "search" or "seizure."[100] Early definitions of a

---

94. U.S. CONST. amend. IV.

95. *See* Riley v. California, 573 U.S. 373, 403 (2014) ("[Supreme Court] cases have recognized that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.").

96. *See id.* (same).

97. *See* Michael W. Price, *Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine,* 8 J. NAT'L SEC. L. & POL'Y 247, 250–58 (2015).

> [A] paramount purpose of the Fourth Amendment was to serve as a guardian of individual liberty and free expression. In other words, it was intended to function as a barrier to government overreach and as a catalyst for other constitutional rights, notably freedom of speech and freedom of association, which are essential to a healthy democracy.

98. *See* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but on probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

99. *See* Weeks v. United States, 232 U.S. 383, 398 (1914) (establishing what eventually became known as the exclusionary rule).

100. U.S. CONST. amend. IV (addressing rights in the context of searches and seizures by the government).

"search" emphasized a physical intrusion into a protected place similar to common-law trespass.[101] In *Olmstead v. United States,* the government's telephone wiretapping did not constitute a search or seizure within the meaning of the Fourth Amendment because the tapping did not physically trespass upon the defendant's property.[102] In contrast, the police's eavesdropping via a "spike mike" electronic listening device violated the Fourth Amendment in *Silverman v. United States* because the device intruded on premises occupied by the defendant.[103] This minor physical trespass amounted to a search even though the spike mike only penetrated several inches into a wall.[104]

In 1967, *Katz v. United States* recognized an intangible sense of privacy that focuses on protecting "people, not places."[105] Rather than analyzing whether the government physically invaded a protected space, the Supreme Court found a search occurs when the government intrudes upon a citizen's reasonable expectation of privacy.[106] In this case, the FBI placed a wire-tap outside of a

---

101. *See* Olmstead v. United States, 277 U.S. 438, 464 (1928) ("The amendment itself shows that the search is to be of material things – the person, the house, his papers or his effects.").

102. *See id.* at 464 ("The [Fourth] Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses of offices of the defendants.").

103. *See* Silverman v. United States, 365 U.S. 505, 509 (1961) (describing the government's actions as "unauthorized physical penetration into the premises occupied by the petitioners").

104. *See id.* at 510–11 (distinguishing this case from previous cases because the wiretap touched the defendant's property).

105. *See* Katz v. United States, 389 U.S. 347, 351–53 ("Once it is recognized that the Fourth Amendment protects people—and not simply 'areas'— against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").

106. *See id.* at 353.

> The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.

public phone booth to record the defendant's call.[107] The Court did not consider whether the phone booth was a constitutionally protected area but whether the defendant sought to keep his conversation private.[108] The defendant was justified in assuming that his phone conversation would remain private when he entered the phone booth and shut the door.[109] *Katz* was a significant decision because the Supreme Court created a new framework for unreasonable searches under the Fourth Amendment. Along with the trespass approach from *Olmstead,* a search occurs when the government invades a "reasonable expectation of privacy" such as listening to a private phone conversation on a public phone booth via a wiretap.[110] Even if the government does not physically touch an individual's property or effects, the government's electronic surveillance can amount to an unreasonable search under the Fourth Amendment.[111]

Justice Harlan offers a two-fold standard in *Katz* to determine whether a reasonable expectation of privacy exists.[112] Courts must consider both a subjective and objective component for this inquiry. An individual must have an actual, subjective expectation of privacy and this expectation of privacy must be "one that society is

107. *See id.* at 348 (stating that FBI agents attached an electronic listening and recording device to the outside of a public telephone booth).

108. *See id.* at 351.

> This effort to decide whether or not a given 'area,' viewed in the abstract, is "constitutionally protected" deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

109. *See id.* at 352 ("One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

110. *See id.* at 353 (deciding the government's electronic listening and recording of the phone booth constituted an unreasonable search under the Fourth Amendment).

111. *See id.* (clarifying that the fact that the listening device did not physically touch the phone booth does not eliminate Fourth Amendment protections).

112. *See id.* at 360–61 (Harlan, J., concurring) ("There is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

prepared to recognize as reasonable."[113] If a citizen has a reasonable expectation of privacy, then the government's actions are considered a search and will typically require a search warrant based on probable cause.

B. An Individual Cannot Invoke Fourth Amendment Protections If the Third–Party Doctrine Applies

One broad exception to the Fourth Amendment occurs when a person who shares information with a third party gives up all constitutionally protected privacy in that information. When a person willingly conveys information to a third party, they assume the risk that the third party will disclose such information to others.[114] This exception, called the "third–party doctrine," originated in the Supreme Court case *United States v. Miller*.[115] In *Miller*, a fire broke out in the defendant's warehouse and officials found a distillery and gallons of non-tax paid whiskey.[116] Subsequently, two banks were subpoenaed and ordered to make the defendant's bank records available to the government.[117] The banks showed an agent microfilm records and provided copies of checks, deposit slips, and financial statements.[118] The Court found no legitimate expectation of privacy in these bank records because the defendant (1) voluntarily conveyed his information to banks in the "ordinary course of business" (2) assumed the risk the information would be conveyed by the bank to the government.[119]

---

113. *See id*. (same).

114. *See* United States v. Miller, 425 U.S. 435, 443 (1976) (stating that the Fourth Amendment "does not prohibit the obtaining of information revealed to a third party" even if the information is revealed for a "limited purpose"); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

115. *See Miller*, 425 U.S. at 443 ("The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . .").

116. *Id.* at 437.

117. *See id.* at 437–39 (describing the government's subpoena for bank records and the defendant's pre-trial motion to suppress the bank records).

118. *Id.* at 438.

119. *See id.* at 442–43 (applying the third-party exception to bank records).

A few years later, the Supreme Court applied the third-party doctrine to personal information, not solely business information, in *Smith v. Maryland*.[120] After a woman was robbed and then received threatening phone calls from a person claiming to be the robber, the police installed a "pen register" on the suspect's home phone without a warrant.[121] The pen register could record all numbers dialed from the defendant's home, but it did not reveal the contents of any call.[122] The register found that the defendant placed a call to the home of the women who was robbed, which was used as evidence when the police obtained a search warrant.[123] The Supreme Court found that the defendant did not have a reasonable expectation of privacy regarding the numbers dialed on his phone because he voluntarily gave the information to a third party—the telephone company.[124] The Court reasoned that "[a]ll telephone users realize that they must convey phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[125]

In *Miller* and *Smith*, the Supreme Court established the third–party doctrine, which provides an exception to Fourth Amendment protections.[126] When an individual voluntarily shares information with a third party, they lose any reasonable

120. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (deciding that the exception applied to a list of phone numbers dialed by the defendant).

121. *Id.* at 737.

122. *See id.* at 741 ("Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.") (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167).

123. *Id.* at 737.

124. *Id.* at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

125. *Id.* at 742.

126. *See id.* at 745–46 (finding that the defendant did not have a reasonable expectation of privacy in bank records because they voluntarily conveyed the records to a third party, the bank); *see also* United States v. Miller, 425 U.S. 435, 443 (1976) (deciding the third-party doctrine applied to the phone numbers that a defendant dialed on a home phone).

expectation of privacy in such information.[127] As stated in *Katz*, an individual must have a reasonable expectation of privacy to assert Fourth Amendment protections against government searches.[128] Thus, if the third–party doctrine applies to a case, the government may search an individual without a search warrant.

C. In Response to New, Advanced Technologies, the Supreme Court Has Recognized Significant Privacy Interests at Stake with Location–Tracking Devices

In *United States v. Carpenter,* the Supreme Court declined to extend the third–party doctrine to historical cell-site location information (CSLI) records from wireless carriers.[129] CSLI refers to "information cell phones convey to nearby cell towers."[130] "Each time a cell phone connects with a cell tower, the time and duration of that connection is recorded by the cell phone service provider."[131] The police in *Carpenter* used historical CSLI information to track a bank robbery suspect's movement during the crimes over a fourth-month period.[132] In two court orders, the government obtained 127 days of CSLI data from MectroPCS and seven days of CSLI data from Sprint, totaling 12,898 location points.[133] While each location point alone could not place the defendant at the crime scenes, the detailed logging of all his movements did determine his

127. *See Miller*, 425 U.S. at 443 (explaining that when an individual willingly shares information with a third party, they assume the risk that the third party will share information with the government); Smith v. Maryland, 442 U.S. 735, 742 (1979) (finding that third-party eliminates any reasonable expectation of privacy and, therefore, Fourth Amendment protections do not apply).

128. *See* Katz v. United States, 365 U.S. 347, 360–61 (1961) (Harlan, J., concurring) (outlining the twofold standard for a reasonable expectation of privacy in Justice Harlan's concurrence).

129. *See* United States v. Carpenter, 138 S. Ct. 2206, 2217 (2018) ("Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.").

130. *See* ELEC. FRONTIER FOUND., CELL SITE LOCATION INFORMATION 1 (March 28, 2019) (providing an overview of cell site location information (CSLI) for criminal defense attorneys).

131. *Id.*

132. *Carpenter*, 138 S.Ct. at 2212.

133. *Id.*

presence at the robbery site.[134] This conceptual framework is often called the "mosaic theory."[135] The Court found that the defendant had a reasonable expectation of privacy in the "whole of his movements." [136]

The Court reasoned that "[m]apping a cell phone's location . . . provides an all-encompassing record of the holder's whereabouts," which "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[137] The Court distinguished between the limited amount of personal information addressed in *Smith* and *Miller* and "the exhaustive chronicle of location information casually collected by wireless carriers today."[138] Moreover, the Court explained that cell phone users do not voluntarily turn over their location to service providers: "a cell phone logs a cell-site record by dint of its

---

134. *See id.* at 2218 ("From the 127 days of location data it received, the Government could, in combination with other information, deduce a detailed log of Carpenter's movements, including when he was at the site of the robberies.").

135. The mosaic theory first appeared in *United States v. Maynard*, the D.C. Circuit opinion later reviewed by the Supreme Court under the name *United States v. Jones*. *See* United States v. Maynard, 615 F.3d 544, 561–62 (D.C. Cir. 2010).

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.

See also Orin S. Kerr, *The Mosaic theory of the Fourth Amendment,* 111 MICH. L. REV. 311, 320–28 (2012) (explaining the mosaic theory's introduction into Fourth Amendment jurisprudence); Robert Fairbanks, *Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-Carpenter,* 26 BERKELEY J. CRIM. L. 71, 76–95 (2021) (examining how lower courts have applied the mosaic theory following *Carpenter*).

136. *See* United States v. Carpenter, 138 S. Ct. 2206, 2218–19 ("[W]hen the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.").

137. *Id.* at 2217 (internal quotation marks and citation omitted).

138. *See id.* at 2219 (contrasting the personal information collected by a cell phone with the much more limited records like bank documents and pen registers).

operation, without any affirmative act on the part of the user beyond powering up."[139] Therefore, the police must generally obtain a warrant supported by probable cause before acquiring historical CSLI records because CSLI technology passively collects revealing, extensive location information on individuals.

Unlike historical CLSI, the Supreme Court has not yet addressed how the Fourth Amendment applies to location data gathered from geofence warrants. Geofence warrants collect location data for every cell phone user within a particular area over a particular span of time.[140] So far, lower courts have considered geofence warrants that law enforcement requests from Google.[141] When law enforcement seek a geofence warrant from Google, it "(1) identifies a geographic area (also known as the 'geofence,' often a circle with a specified radius), (2) identifies a certain span of time, and (3) requests Location History data for all users who were within that area during that time."[142] Google "Location History" may collect users' location information from various sources, including from "Global Positioning System ('GPS') information, Bluetooth beacons, cell phone location information from nearby cellular towers, Internet Protocol ('IP') address information, and the signal strength of nearby Wi-Fi networks."[143] Google stores all this location data in a repository known as the "Sensorvault," where each device receives a unique device ID.[144] Although Google transforms this aggregated data to not appear as individual user

139. *Id.* at 2220.

140. *See* Haley Amster & Brett Diehl, Note, *Against Geofences,* 74 STAN. L. REV. 385, 388 (2022) ("Geofence warrants proceed first by giving investigators access to data for all cellular devices that were present near a crime scene around the time when the crime occurred.").

141. *See In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning Arson Investigation, 497 F. Supp. 3d 345, 363 (N.D. Ill. 2020) (finding the geofence warrant was "sufficiently particular" when it was limited in time and location); *In re* Search of Info. That Is Stored at Premises Controlled by Google, LLC, 542 F. Supp. 3d 1153, 1158 (D. Kan. 2021) (finding a geofence warrant was overly broad); United States v. Chatrie, 590 F. Supp. 3d 901, 929 (Va. E.D. 2022) (finding a geofence warrant was not particular enough because the government lacked probable cause for each person captured in the geofence warrant).

142. *Chatrie*, 590 F.3d. at 914.

143. *Id.* at 908.

144. *See id.* at 908 ("Google stores this [location] data in a repository known as the 'Sensorvault' and associates each data point with a unique user account.").

data and uses it for advertising and marketing purposes, Google can alter the data back to identify users in response to geofence warrant requests from police.[145]

Since Google policy requires law enforcement to issue a warrant to receive geofence location data, lower courts have focused their decisions on the warrant's particularity and overbreadth requirements, rather than determine whether users maintain a reasonable expectation of privacy in geofence location data. For example, in *United States v. Chatrie*, the Virginia Eastern District Court held that 17.5 acre (more than three football fields) geofence warrant for an urban area violated the Fourth Amendment because the government lacked particularized probable cause to search every person within the area.[146] Although this *Chatrie* holding did not answer whether the defendant had a reasonable expectation of privacy in data sought by the geofence warrant, the Court expressed a "deep concern" with the *Katz* test and third-party doctrine, suggesting current Fourth Amendment doctrine is substantially behind technological innovations.[147] The Court highlights the disturbing way geofence warrants gain access to a previously unknowable category of information.[148] The "expansive, detailed, and retrospective nature" of Google location data allows police to retrace a person's whereabouts without even knowing in advance who they want to follow.[149]

---

145. *See id.* ("Google then builds aggregate models within the Sensorvault with data that is transformed so that it no longer looks like user data. Clearly, however, Google can alter the data back to identify users in response to a geofence warrant.").

146. *See id.* at 930 ("[The geofence warrant] swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny.").

147. *See id.* at 925 ("As Fourth Amendment law develops in a slow drip, 'technology continues to enhance the Government's capacity to encroach upon areas normally guarded from inquisitive eyes.'") (quoting Carpenter v. United States, 138 U.S. 2206, 2214 (2018)).

148. *See id.* ("Until recently, the ease with which law enforcement might access such precise and essentially real-time location data was unimaginable.").

149. *See id.* ("It is this expansive, detailed, and retrospective nature of Google location data that is unlike, for example, surveillance footage, and that perhaps causes such data to 'cross the line from merely augmenting [law enforcement's investigative capabilities] to impermissibly enhancing' them.").

IV. The Fourth Amendment Does Not Currently Offer Significant Protections for Either the Personal Information Stored on Femtech Apps or the Location Data That Companies Like Fog Data Sell to Authorities

The Fourth Amendment fails to protect all the personal information listed in Part II.[150] Whether a femtech user shares their personal health data publicly or preserves it for their eyes only, the Fourth Amendment does not safeguard their data from the government. Femtech companies can share private information with law enforcement and data brokers due to the third-party doctrine. Third-party companies such as Fog Data can also sell location data directly to law enforcement agencies with no restrictions whatsoever.

A. The Fourth Amendment Does Not Protect Public Nor Private Information Electronically Stored on Femtech Apps

1. Femtech Users Cannot Invoke Fourth Amendment Protections for Information Shared on Public Forums

The Fourth Amendment does not provide any privacy protections for femtech community forums because users share their information publicly on these platforms. *Katz* established that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[151] When a person posts a comment or picture on a forum, they "knowingly expose" their content to the public, which means they do not expect their information will remain private.[152] Similarly, "social media users have no reasonable expectation of privacy in their social media postings—even if users communicate their information behind password-protected pages."[153] Just as

150. *See supra* Part II. (describing the information femtech apps collect from users).

151. Katz v. United States, 389 U.S. 347, 351 (1967).

152. *See id.* (connecting a person's actions with their expectation of privacy).

153. Brian Mund, *Social Media Searches and the Reasonable Expectation of Privacy*, 19 YALE J. L. & TECH. 238, 240 (2017).

public posts on Facebook or Instagram convey no intention of privacy, femtech users do not intend to keep their communications private when they deliberately share stories and images on community forums to connect with other women. Thus, Fourth Amendment protections do not apply to community forums on femtech apps because users lack a reasonable expectation of privacy. Law enforcement may search these public forums without a search warrant and freely investigate whether women obtained illegal abortions.

2. The Third-Party Doctrine Allows Femtech Companies to Evade Fourth Amendment Protections for Privately Stored Information

Even if a woman seeks to keep their health information private on a femtech app, the Fourth Amendment will likely not protect them. A femtech user could take advantage of all possible privacy settings on their phone—including password protection, an "anonymous mode,"[154] or encryption—and still not be covered under the Fourth Amendment.[155] Under current jurisprudence, the Fourth Amendment fails to protect the private information collected and sold on femtech apps because the third-party doctrine eliminates any reasonable expectation of privacy.

To determine whether the third-party doctrine applies to digital data and internet service providers, courts consider whether a company's terms of use notify users that the company will share personal information with law enforcement. In *Smith*, the Supreme Court noted that the telephone company's policy stated it used pen registers to detect and prevent violations of the law and to check for obscene, troubling calls.[156] Similarly, lower

154. *See Flo Privacy Policy, supra* note 51 (describing an app feature purported to increase user privacy).

155. *See* Mund, *supra* note 153, at 240 ("The law treats these 'private' social pages as deserving the same protections as if they were publicly posted on the internet.").

156. *See* Smith v. Maryland, 442 U.S. 735, 742–43 (1979) ("Most phone books tell subscribers, on a page entitled 'Consumer Information,' that the company 'can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.'").

courts considering digital data often examine a company's privacy policies and terms of service to eliminate expectations of privacy according to the third-party doctrine.[157] Most lower court cases find that as long as a "policy disclosed the collection, retention, or use of an individual's data, that the user was charged with knowledge of that disclosure and with a commensurate lack of expectation that their data might remain private at all."[158] Courts have consistently held that an individual retains no expectation of privacy in subscriber information, such as IP addresses and related information.[159] This common understanding among courts regarding subscriber information remained after *Carpenter*.[160]

While app users do not have a reasonable expectation of privacy in "non-content" information, such as IP addresses, they may theoretically retain privacy interests in electronically stored "content" information.[161] One of the country's foremost scholars of the Fourth Amendment, Professor Orin Kerr, compares terms of service to consenting to a rental agreement.[162] He believes consenting to terms of service does not eliminate an expectation of privacy but concedes that "agreeing to Terms of Service may in

157. *See* Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357, 1392 (2019) ("Lower courts, applying the strong pre-*Carpenter* third-party principle to emerging digital technologies, often turned to privacy policies and terms of use to discern whether users had 'voluntarily conveyed' or 'knowingly expose[d]' their data to third-party collection.").

158. *Id.*

159. *See* United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (concluding the defendant did not have a reasonable expectation of privacy in his internet and phone subscriber information, such as his name, email address, telephone number, and physical address).

160. *See* United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018) (finding that IP addresses and related information remain "comfortably within the scope of the third-party doctrine" because such information "had no bearing on any person's day-to-day movement' and an individual 'lacked a reasonable expectation of privacy in that information.').

161. *See* Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STANFORD L. REV. 1005, 1018 (2010) (suggesting that electronic communications should be differentiated according content and non-content information, similar to the physical distinction between inside and outside employed in traditional Fourth Amendment jurisprudence).

162. *Id.* at 1031 n.100 ("The breach of Terms of Service should not eliminate a reasonable expectation of privacy in an Internet account for the same reasons that the breach of a rental agreement in an apartment does not itself eliminate a tenant's reasonable expectation of privacy.").

some cases confer rights on the provider to access the contents of the account or consent to a law enforcement search."[163] In practice, the content/non-content distinction does not offer stronger privacy protections because private companies can easily share sensitive data with police, as long as they include this possibility—that they may comply with law enforcement—in their terms of service. All of the femtech apps considered in this Note seize on this third-party exception to the Fourth Amendment. Each femtech app states in their terms of service that they will respond to law enforcement requests and share personal user data, including highly sensitive health and wellbeing data.[164] Therefore, femtech companies can evade Fourth Amendment protections against government intrusion by simply providing "notice" in their terms of service—even if this language is embedded in thousands of pages of convoluted policies.[165]

B. Fog Data Services Evade the Fourth Amendment's Longstanding Goal to Prevent Unfettered Government Surveillance.

Even though Fog Data's location tracking services are extremely similar to the types of surveillance technologies the courts are restricting the government from using, judges have yet to explicitly extend Fourth Amendment protections to the data police can collect from Fog Data. Law enforcement can perform two types of searches on the Fog Data platform: device searches and a

163. *Id.*

164. *See My Calendar Privacy Policy, supra* note 52 ("If we are required to, we may also use your Personal Information to respond to a valid and enforceable court order, law, or legal process."); *Flo Privacy Policy, supra* note 51 (allowing the company to share personal data "in response to subpoenas, court orders or legal processes, to the extent permitted and as restricted by law"); *Glow Privacy Policy*, *supra* note 50 ("We may use your personal information to: comply with applicable laws, lawful requests, and legal process, such as to respond to subpoenas or requests from government authorities."); *BabyCenter Privacy Policy*, *supra* note 51 ("We may disclose your User Information to legal and regulatory authorities (including law enforcement agencies and courts) to respond to legal requests or orders, comply with applicable law, or exercise or defend our legal rights.").

165. *See BabyCenter Privacy Policy*, *supra* note 51 (providing an 8,500-word document for its terms of service).

geofencing-equivalent Reveal function.[166] If the police have a known advertising ID, they perform a "device search" in Fog Data's database to trace that device's precise location over months or even years.[167] A device search on Fog Data is similar to the historical CSLI in *Carpenter* because both technologies track location data points overtime and are associated with one mobile device. Additionally, Fog Data's Reveal feature performs a dragnet search equivalent to a geofence warrant; it identifies all devices within a certain area and time and then does a "pattern-of-life analysis" to identify the owner of each device.[168] This "pattern of life analysis" can reveal where suspects work, live, and associate.[169] Fog Data's Reveal feature is essentially a geofence warrant under a different name because both surveillance techniques draw a shape around a crime scene and designate which mobile devices were present at any given time.[170]

Although the Fog Data device search is similar to CSLI and Fog Data Reveal is the equivalent to geofence warrants, the courts have not explicitly extended Fourth Amendment protections to this type of company. Law enforcement subscribers to Fog Data do not have consistent policies about whether police should seek a search warrant before using Fog Data's massive database.[171] California agencies direct police to seek warrants "unless exigent circumstances exist" but the police did not always adhere to this

166. *See* Guariglia, *supra* note 90 ("[Police] can draw a box and see identifiers representing every device within that geographical area at a given time frame. They can also use a device's ID to trace that device's precise location history over months or even years.").

167. *See* Guariglia, *supra* note 90 (explaining how police use Fog Data device searches to track individuals).

168. *See* Cyphers, *supra* note 89 (illustrating how Fog Data services provide a comprehensive analysis and record of individual behavior over time).

169. *See Data Broker Helps Police See Everywhere You've Been with the Click of a Mouse*, *supra* note 93 (revealing the personally identifying nature of Fog Data's location data).

170. *See* Cyphers, *supra* note 89 ("Fog's 'Reveal' feature can also be used to execute a dragnet search of large physical areas in what is the equivalent of a 'geofence warrant.'").

171. *See id.* (explaining how some police departments will involve the court and obtain a warrant before using Fog Data while others will use the paid services completely independently).

policy.[172] Tennessee Bureau of Investigation and Indiana State Police said the police could use Fog Data to conduct area searches without a warrant but required them to get a warrant for device searches and pattern-of-life analysis.[173] Many other police departments believed Fog Data required no "paperwork" or warrant for any services.[174] The inconsistent understandings and practices among local police regarding Data Fog demonstrate the need for judicial or legislative clarification.

Since other data brokers have already sold location data at Planned Parenthood with advertisers, it is not a far leap to consider that Fog Data may sell location data on abortion clinics with law enforcement. The data broker SafeGraph classifies Planned Parenthood as a "brand" that can be tracked, and its database includes more than 600 Planned Parenthood locations in the United States.[175] In total, it costs around $160 for a week's worth of data on where people who visited Planned Parenthood came from, and where they went afterwards.[176] Fog Data could sell location data on abortion clinics just like SafeGraph, but this information would be even more damaging in the hands of police. In a hypothetical situation in which the police are investigating an illegal abortion, the police could use Fog Data in two ways: perform a device search for a known device or draw a dragnet feature around an abortion clinic. Police would use the device search feature later in an investigation when they already know their suspect and want to confirm the suspect visited an abortion clinic. Alternatively, the dragnet, or geofence, feature would allowed the police to search a clinic without any known suspects. After

172. *See id.* ("Some California agencies sought warrants at least some of the time that they used Fog.").

173. *Id.*

174. *See id.* ("A Maryland State Police sergeant wrote, erroneously, that Fog 'requires no paperwork since it's data you get from a company and has no [personally identifying information] etc.'").

175. *See* Bennett Cyphers & Gennie Gehart, *SafeGraph's Disingenuous Claims About Location Data Mask a Dangerous Industry*, ELEC. FRONTIER FOUND. (May 6, 2022) (questioning whether SafeGraph actually "only sell[s] data about physical places (not individuals)") [perma.cc/8GEW-SF3Y].

176. *See id.* (finding SafeGraph's claims misleading because it previously sold data about individuals and because the information it now sells is "based on the same sensitive, individual location traces that are collected and sold without meaningful consent").

discovering which devices were at certain abortion clinic at a certain time, police could perform Fog Data's pattern-of-life analysis to potentially uncover who owns the phone and, thus, attended the clinic.

V. Judicial Solutions

A. The Courts Should Reconsider the Third Party Doctrine Within the Context of Modern Femtech Apps

A new judicial approach is needed to evaluate Fourth Amendment protections for femtech apps. As described in Subpart IV.A., courts currently rely on a "notice-and-consent privacy regime" to determine if the third-party doctrine applies to electronically stored information.[177] As long as a femtech app includes "notice" their terms of service or privacy policy that they will share user information with third parties and/or law enforcement, the third-party doctrine will eliminate any expectation of privacy.[178] Thus, the third party doctrine essentially removes Fourth Amendment protections for information on most femtech apps because femtech companies easily include these "notice" provisions in their policies. To improve privacy protections for femtech users, the courts do not have to remove the third-party doctrine entirely. Instead, the courts should reconsider *how* the third-party doctrine applies to femtech apps, grappling with the meaning of consent and voluntariness in a more complicated digital age.

According to *Miller* and *Smith*, the third-party doctrine is triggered when individuals voluntarily convey information to another and assume the risk that such information may be shared with the government.[179] I propose a new judicial approach to the third-party doctrine that centers meaningful user consent. The

177. *See* Michael Gentithes, *App Permissions & The Third-Party Doctrine,* 59 WASHBURN L.J. 35, 50 (2020) (describing the main critiques of notice-and-consent privacy regimes).

178. *See supra* Subpart IV.A.2. (explaining how third party doctrine allows femtech apps to easily circumvent Fourth Amendment privacy protections).

179. *See supra* Subpart III.B. (outlining the fundamental cases and principles of the third party doctrine in Fourth Amendment jurisprudence).

third-party doctrine should not apply to electronically stored information on femtech apps unless a user genuinely consents to convey such information to the app. Genuine consent should require sufficient knowledge, voluntariness, and a manifestation of consent.

In "The Fragility of Consent," Lori Andrews identifies these requirements for an app user to properly consent to a company's policy: (1) knowledge, (2) voluntariness, and (3) manifestation of consent.[180] Knowledge refers to "sufficient understandable information to provide the foundation for true consent."[181] Voluntariness requires intention and must be free of "undue pressure or coercion."[182] And manifestation of consent must be an explicit expression, not simply implied.[183] For example, visiting a surgeon's office does not mean that you consent to whatever surgery she proposes.[184] In the same vein, opening a femtech app should not mean users automatically consent to the collection of their private information for marketing purposes or to the sale of their advertising IDs, and other location identifiers, to data brokers.[185]

Femtech privacy policies do not provide adequate information upon which to base a decision about whether to use the app. Their privacy policies are often difficult to understand or even incomprehensible, preventing a user from gaining enough knowledge to provide valid consent.[186] An average consumer will

180. *See* Lori Andrews, *The Fragility of Consent*, 66 LOY. L. REV. 11, 12 (2020) (outlining the conditions that would provide for proper informed consent in using mobile apps).

181. *Id.*

182. *Id.*

183. *See id.* at 12 ("[The manifestation of consent] must be explicit, rather than implied.").

184. *See id.* (illustrating the absurdity of "consenting" to broad privacy policies without knowing what the terms are or what they mean).

185. *See id.* at 12–13 ("[M]y use of an app [should not] mean that I consent to the collection of my private information for marketing purposes, to the activation of the microphone on my phone, or to the use of cookies or other tracking mechanisms to collect information . . . .").

186. Mark Rowan & Josh Dehlinger, *A Privacy Policy Comparison of Health and Fitness Related Mobile Applications*, 37 PROCEDIA COMPUT. SCI. 348, 354 (2014) (analyzing the readability of privacy policies of 20 health-related apps and concluding that the policies lacked transparency).

not understand the technical or legalese language that permeates these policies. The average reading level of health app privacy policies is above the twelfth-grade level.[187] Meanwhile, the average American adult reads at 7th to 8th grade reading level, 54% of adults read below a sixth-grade level, and 21% of adults are illiterate.[188] Moreover, privacy policies may deliberately use terms that obscure how femtech apps use information.[189] For example, "saying that an app only shares information with 'affiliates' and 'third-party service providers,' may give users the impression of only sharing data with a small group. However, 'affiliates' and 'third parties' can mean any entity that pays the app developer for user's information."[190] One study of 20 popular health apps found that although each app shared personal user information with third parties, their privacy policies discussed data retention and sharing procedures in vague terms or not at all.[191] Most apps in this study did not state why they collected this data nor whom they shared information with.[192] If an average consumer cannot fully understand the terms or implications of a privacy policy, they do not have enough information to voluntarily consent.

An average femtech user may also have flawed assumptions or misconceptions when reading and "consenting" to privacy policies. A "consumer might assume that the existence of a privacy statement means that their private information would be protected."[193] However, having a privacy policy does not mean an app protects an individual's privacy, and "apps with privacy policies [are] slightly more likely to disclose information to third

187. *Id.*

188. Sandra Craft, *Literacy Statistics,* THINKIMPACT (Oct. 16, 2023) [perma.cc/6MPF-FCBD].

189. *See* Andrews, *supra* note 180, at 12 (stating that their study of health apps "found that the privacy policies were sometimes difficult to understand or even incomprehensible").

190. *Id.* at 14.

191. *See* Rowan, *supra* note 187, at 353 ("Only a few applications addressed end user procedures for personal data access or correction. . . . In addition, data retention procedures were rarely reported.").

192. *See supra* Subpart II.C. (explaining how My Calendar and Flo disclose which third parties they share information with, while Glow and BabyCenter do not disclose their partners).

193. Andrews, *supra* note 180, at 16.

parties than those without privacy policies."[194] Femtech apps can be especially confusing for consumers because users might assume that the health information collected is protected by the privacy rules adopted pursuant to HIPAA, the Health Insurance Portability and Accountability Act.[195] Yet, femtech apps do not qualify as a "covered entity" under HIPAA and, therefore, can still gather, store, and sell health information about individuals.[196]

Even if a consumer can read and understand all the terms in an app's privacy policy, the policy may not share accurate or complete information. In a study assessing hundreds of medical apps, researchers compared what the apps' privacy policies said their apps did with what the apps actually did.[197] "Some apps said they would not share user information with third parties, yet they did. Other apps said they would encrypt information, but they did not."[198] Thus, regardless of what a privacy policy claims, people do not genuinely know whether femtech apps will protect their data or share their personal information with third-parties. For example, Flo and My Calendar's privacy polices tried to limit which user data is shared and disclosed which third parties they partner with.[199] But this study suggests that users cannot not fully trust Flo or My Calander's policies because, in practice, the apps could breach their own terms, either sharing more information or partnering with more third parties than users originally agreed to.

Without sufficient knowledge, people cannot voluntarily choose to share data with femtech apps. The inaccessibility, incomprehensibility, and inaccuracy of privacy policies prevent

194. *Id.*

195. *See id.* at 15 (discussing reasonable misunderstandings of an app's privacy guarantees).

196. *See* EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA, U.S. DEP'T OF HEALTH & HUM. SERVS 7–11 (examining how HIPAA does not address new technologies like wearable health devices, mobile applications, and social media sites).

197. *See* Andrews, *supra* note 180, at 13 (describing the scope and purpose of their study).

198. *Id.* at 15.

199. *See supra* Subpart II.C. (identifying Flo and My Calendar's efforts to protect user privacy on their apps).

users from obtaining the information needed to give valid, voluntary consent.[200]

Furthermore, voluntary consent is undermined when femtech apps do not request or require manifestation of user consent. While some femtech apps ask users to click a box to demonstrate their consent to a policy, others simply assume that people agree when they use the app.[201] And most users will click "okay" to requests without ever opening or reading a privacy policy.[202] Given the numerous apps that people use on a daily basis, "it is not humanly possible to read, process, and apply all the privacy policies with which a modern individual comes in contact."[203] The average person has at least 80 apps downloaded on their smartphone,[204] and reading the privacy policies for 80 apps would take approximately 22.4 hours to read.[205]

Even if a user takes the time to read a privacy policy and affirmatively communicates their agreement via a "click," or

200. *See* Andrews, *supra* note 180, at 21 ("The legal standard for consent is not being met in the apps context. Knowledge is insufficient, coercion has replaced voluntariness, and consent is not adequately manifested.").

201. *See* Glow, Mobile Application (Version 9.9.22, 2023) (prompting users to agree, via a click of a button, to their terms and privacy policy after installing the app); My Calendar – Period Tracker, Mobile Application (Version 8.7.0, 2023) (providing a link to learn more about their privacy policy when setting up an account but not requiring any affirmative action to demonstrate consent); Flo Period and Pregnancy Tracker, Mobile Application (Version 9.34, 2023) (requiring that, upon installation, users to click boxes saying they agree to Flo's privacy policy and terms of use); Pregnancy Tracker – Baby Center, Mobile Application (Version 4.36.1, 2023) (listing a small statement that by registering for an account, users are automatically agreeing to their privacy policy and terms of use).

202. *See* Andrews, *supra* note 180, at 17 (critiquing the idea that users genuinely manifest consent to apps' privacy policies); Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information* PEW RSCH. CTR. (Nov. 15, 2019) ("97% say they are ever asked to approve privacy policies, yet only one-in-five adults overall say they always (9%) or often (13%) read these policies.") [perma.cc/X6E8-SFX6].

203. *Id.*

204. *See* Susan Laborde, *Mobile App Statistics Everyone Should Know in 2023,* TechReport (July 27, 2023) (presenting various statistics for mobile apps in 2023) [perma.cc/3UZ7-N79K].

205. *See* Geoffrey A. Fowler, *I tried to read all my app privacy policies. It was 1 million words.* WASHINGTON POST (May 31, 2022) (providing a calculator to determine the number of words and hours required to read the privacy policy of a given amount of mobile apps) [perma.cc/6FXK-V629].

another method, bait-and-switch tactics often eliminate this initial manifestation of consent.[206] App developers do not make commitments to honor the policies in place at the time a user originally installs or signs up for the app.[207] Some femtech apps' policies say they give rise to no rights, while others say that they can change their terms at any time.[208] None of the apps state they will email individuals and ask whether they agree to new terms.[209] Rather, users are responsible for continuously monitoring app's website to look for changes in their privacy policy.[210] Consequently, people must read a privacy policy in its entirety and figure out what changed.[211] A person would have to invest another thirty days each time they reviewed and looked for changes in the privacy policies of their commonly used apps.[212] As Lori Andrews points out, "When will you sleep or work?"[213]

Under this three-part framework for consent, femtech users would retain Fourth Amendment protections because the third

206. *See* Andrews, *supra* note 180, at 18 (referencing the fact that privacy policies can change at any time).

207. *See id.* at 19 ("Seventy-three percent of the bipolar apps we studied said that the terms of their privacy policy could be changed at any time. None of them said that they would definitely email the person and give her the choice of whether to agree to the new terms.").

208. *See BabyCenter Privacy Policy*, *supra* note 51 ("This Policy may be amended or updated from time to time . . . We encourage you to read this Policy carefully, and to regularly check this page to review any changes we might make."); *Glow Privacy Policy*, *supra* note 50 ("We reserve the right to modify this Privacy Policy at any time.").

209. *See BabyCenter Privacy Policy*, *supra* note 51 (placing the responsibility on users to continually review the privacy policy for any changes); *Flo Privacy Policy, supra* note 51 ("Your continued use of the Services after the effective date of an updated version of the Privacy Policy will indicate your acceptance of the Privacy Policy as modified."); *Glow Privacy Policy*, *supra* note 50 ("In all cases, your use of the Service after the effective date of any modified Privacy Policy indicates your acceptance of the modified Privacy Policy.").

210. *See* Andrews, *supra* note 180, at 19 (emphasizing how difficult it is for app users to stay informed about updates to privacy policies).

211. *See id.* ("A few apps' privacy policies that we studied states that they would change the date when there is a new policy, but none said they would highlight the changed portion.").

212. *See id.* at 20 ("That's another thirty days each time you have to inventory the privacy policies of the apps and digital services you commonly use. And you are advised to do that complete review 'frequently' or 'often.'")

213. *Id.*

party doctrine would no longer apply. There would be a heightened standard to eliminate Fourth Amendment protections via the third-party doctrine. The third-party doctrine would only be triggered if a person *genuinely consented* to give their information to a third party, and genuine consent would demand a showing of knowledge, voluntariness, and manifestation of consent. Currently, femtech apps do not satisfy any of these necessary elements for consent, which means users are not voluntarily consenting to these privacy policies that give companies free reign to sell data, and, thus, users should retain their expectations of privacy under the Fourth Amendment.

B. The Courts Should Extend Carpenter's Reasoning to Fog Data's Dragnet Surveillance Technology

Along with redefining consent within the third-party doctrine, courts should consider how *Carpenter* applies to data broker companies who employ geofencing technology, such as Fog Data. The Supreme Court's concerns from *Carpenter* are reflected in Fog Data's location-tracking techniques because the company's database offers the government "an intimate window" into an unlimited number of people's lives at a low cost.[214]

The courts should extend the principles from *Carpenter* to the extensive location data Fog Data collects and shares with police without an individual's knowledge or consent. Police should have to obtain a warrant to use either Fog Data's device search or area search (a geofencing technique). Expanding Fourth Amendment protections for more location technologies like Fog Data will be important for women's reproductive privacy because then the police will not have such easy access to identify and investigate people traveling to receive abortion care.

Fog Data's device search provides a more detailed picture of a person's life than CSLI. In *Carpenter*, cell phone carriers provided

214. *See* United States v. Carpenter, 138 S. Ct. 2206, 2217 (2018) ("As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'").

the government with 12,898 data points over 127 days.[215] In one Missouri case, Fog Data provided 47,394 signals over 163 days for a single phone.[216] Just as historical CSLI data provides an "intimate window into a person's life,"[217] Fog Data surveillance "not only includes possible crime scenes, but also homes, churches, workplaces, health clinics, or anywhere else."[218] Nor do people knowingly or willing give their location data to Fog Data or the police who use Fog Data. Rather, people automatically allow smartphone apps like femtech apps to have access to their advertising IDs by "consenting" to the company's privacy policy. Yet no reasonable person expects this will result in the app tracking all their movements, the app selling this sensitive information to a data broker, and the police ultimately buying it.

Fog Data founder, Robert Liscouski, argued that *Carpenter* does not apply to their data because the "original advertising ID is hashed and anonymized" so the company "cannot identify an individual based on the hashed ID."[219] However, this claim that Fog Data's information is anonymous is simply not true. It is nearly impossible to anonymize location data because the "whole of a person's movements" can reveal a lot about their private life.[220] One study found researchers could identify 50% of people using

215. *See id.* at 2212 (noting the extensive amount of information historical CSLI gathers).

216. *See* Cyphers, *supra* note 89 (comparing the amount of location information in *Carpenter* to Fog Data's massive database).

217. *Carpenter*, 138 U.S. at 2217.

218. *Data Broker Helps Police See Everywhere You've Been with the Click of a Mouse*, *supra* note 93.

219. Cyphers, *supra* note 89.

220. *See* United States v. Maynard, 615 F.3d 544, 561–62 (D.C. Cir. 2010) ("The whole of one's movements over the course of a month is not constructively exposed to the public baron ecause, like a rap sheet, that whole reveals far more than the individual movements it comprises."); *see also* United States v. Jones, 565 U.S. 400, 403 (2012) (explaining how the Government used GPS-derived locational data to connect defendant "to the alleged conspirators' stash house that contained $850,000 in cash, 97 kilograms of cocaine, and 1 kilogram of cocaine base"); *see also* United States v. Carpenter 138 U.S. 2206, 2218–19 (2018) ("[W]hen the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.").

two random time and location points.[221] Meanwhile, Fog Data gives police access to billions of location data points on its database. As a whistleblower and former police officer in North Carolina expressed, "if police could not use this number to identify the owner, it would be of no use to them. In fact, this information can be used to determine the identities of anyone captured in the initial search."

Along with the parallels to *Carpenter*, Fog Data services replicate problematic surveillance themes that suggest a reasonable expectation of privacy should exist for this advanced technology. For example, Matthew Tokson identified three consistent principles that drive the Supreme Court's assessments of Fourth Amendment privacy: "the intimacy of the place or thing targeted; the amount of information sought; and the cost of the investigation."[222] Intimacy "refers to the personal or sensitive nature of a thing, and to qualities associated with close, familial, or romantic relationships with others."[223] Amount refers to the number of bits of information on a suspect the police seek and ultimately gather and store.[224] The Supreme Court is more concerned about privacy violations when a technology reveals greater intimacy and amount of data. Finally, cost concerns "the time and effort required for police officers to effectuate a surveillance practice" and is most salient when the cost is particularly high or low.[225] The Supreme Court is concerned about a technology if the government can gather a large amount of

221. *See* Cyphers, *supra* note 89 ("It is impossible to anonymize location data, because it reveals unique patterns of movement that are trivially easy to link to identifiable people.").

222. *See* Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 13–27 (2020) (synthesizing principles that have "likely shape[d] judicial intuitions regarding the severity of a surveillance practice and the need for constitutional regulation").

223. *Id.* at 15.

224. *See id.* at 18 ("In practice, the amount of information sought will typically be measured by the

extent and duration of a surveillance practice, or how much information about a suspect is ultimately obtained and stored.").

225. *Id.* at 22.

information at a low cost, especially when the surveillance is "scalable and easily applied to large groups of citizens." [226]

All three of these problematic surveillance principles—(1) intimacy, (2) amount, and (3) cost—are present with Fog Data services. As described above, Fog Data allows police to search billions of location data points, and its "pattern of life" analysis reveals highly intimate information about a person's behaviors, beliefs, and daily practices. If law enforcement launched a Fog Data geofence search around a women's health clinic, this surveillance would intrude upon a woman's "close relationships," including her family and doctor-patient relations.[227] Finally, the cost of using Fog Data is low for police and is particularly concerning because the surveillance technology is "easily applied to large groups of citizens."[228] Rather than paying for officers to stake out in front of a clinic all day and night for weeks or months, local police departments can simply pay a onetime subscription fee to Fog Data and instantly track everyone who enters a women's health clinic.[229] Therefore, the courts should recognize that a reasonable expectation of privacy exists for the location information Fog Data collects and sells to police due to the intimate nature of the data, the massive amount of data, and the extremely low cost to police.

VI. Congress Should Strengthen Individual Privacy Rights for Health and Location Data

One issue with relying on the courts to expand *Carpenter* principles is that the courts move slowly to address each case, especially cases that work their way up to the Supreme Court. By the time the Supreme Court addresses geofencing or data brokers,

226. *See id*. at 23. ("Cost is an important component of reasonable expectations of privacy because it impacts both the extent and the validity of government surveillance.").

227. *See id*. at 15 (explaining the intimacy aspect of Fourth Amendment privacy as it concerns familial relationships and other close and personal bonds).

228. *See id.* at 23 ("As practical barriers to government observation are eliminated by new, low-cost surveillance methods, the potential for exposure of private information to the government sharply increases.").

229. *See* Cyphers, *supra* note 89 (noting that police departments already have access to Fog Data).

police might be using new a more advanced surveillance technologies to track suspects. Courts' decisions are also limited by the facts of the single case before them.[230] For example, the Supreme Court was careful to limit their holding in *Carpenter* to historical CSLI and did not address how the Fourth Amendment applies to real time CSLI, "tower dumps," or other location-tracking techniques.[231] In *Jones*, a case dealing GPS monitoring, Justice Alito noted, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[232] Thus, Congress may be better equipped to deal with surveillance technologies because the legislature can pass comprehensive statutes that solve the most current, pressing privacy issues.

The legislature can create comprehensive laws to protect personal health information stored on new technologies like femtech apps. One avenue to strengthen privacy rights is to expand HIPAA coverage beyond its narrow, outdated covered entities.

Health Insurance Portability and Accountability Act (HIPAA) and its associated administrative rules protect the privacy of personal health information.[233] HIPAA prohibits healthcare providers and businesses from disclosing protected information to anyone other than a patient without consent.[234] HIPAA gave the U.S. Department of Health and Human Services (HHS) authority to develop rules protecting the confidentiality of personal health

230. *See* Sup. Ct. R. 14.1(a) ("Only the questions set out in the petition, or fairly included therein, will be considered by the Court.").

231. *See* United States v. Carpenter, 138 U.S. 2206, 2220 (2018) ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval).").

232. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring) (internal citation omitted).

233. 45 C.F.R. § 164.508 (2022).

234. *See id.* at (a)(1) ("Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section.").

information.[235] As a result, HIPAA rules grant individuals several rights regarding their health information, "including access to information, ability to demand an accounting of certain disclosures, and some control over how the information is used and shared."[236]

Although HIPAA "stands out in the American mind" as a strong safeguard for healthcare information, HIPAA restricts "only a small subset of health care industry disclosures."[237] HIPAA protects health information based on the type of entity holding the information rather than the characteristics of the information itself.[238] HIPAA applies only to "covered entities" and their business associates.[239] Covered entities refers to "a health plan, health care clearinghouse, [or] a health care provider."[240] More and more organizations, including femtech apps, fall outside the scope of HIPAA but still gather, store, and transmit health information about individuals.[241] Further legislation is needed to ensure

235. *See* Matthew T. Bodie, *HIPAA*, 2022 CARDOZO L. REV. DE NOVO 118, 120 (2022) ("The Act tasked the U.S. Department of Health and Human Services (HHS) to develop protocols protecting the confidentiality of personal health information.").

236. *Id.*; *see also* U.S. DEP'T HEALTH & HUM. SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 13 (2016).

> [HIPAA] enforces: the HIPAA Privacy Rule, which protects the privacy of protected health information in the hands of HIPAA covered entities and their business associates; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; and the HIPAA Breach Notification Rule, which requires covered entities to provide notification following a breach of unsecured protected health information.

237. *See* Bodie, *supra* note 235 at (discussing the misuse of HIPAA in common language and privacy rights claims).

238. *See Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA*, *supra* note 236, at 12 ("[I]n the health sector, the current federal laws protect an individual's health information based upon the type of entity holding the information rather than solely upon characteristics of the information itself.").

239. *See* 45 C.F.R. § 160.103 (defining covered entity and business associate).

240. *Id.* (formatting removed).

241. *See Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA*, *supra* note 236, at 7–11 (analyzing how HIPPA does not address new technologies like wearable health devices, mobile applications, and social media sites).

sensitive health information on femtech apps is covered under HIPAA.

In 2016, HHS and the Federal Trade Commission sent a report titled "Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA" to Congress, urging the legislatures to adopt modern protections for personal health data.[242] This report focuses on health tracking technologies—such as wearable fitness devices, social media sites, and mobile health apps—that are common today but are not covered by HIPAA (referring to these technologies as "non-covered entities").[243] The report identifies many of the main privacy concerns resulting from unregulated health technologies (including femtech apps). These "non-covered entities" have long, convoluted privacy policies and freely share health information with advertisers and third parties.[244]

One potential way to expand HIPAA protections is to enact the proposed Protecting Personal Health Data Act.[245] This bill would require the promulgation of agency regulations to help strengthen privacy and security protections for consumers' personal health data not previously covered by HIPAA.[246] The HHS Secretary would improve privacy protections for health data "that is collected, processed, analyzed, or used by consumer devices, services, applications, and software."[247] The term "consumer devices, services, applications, and software" includes mobile technologies and social media sites designed to collect individuals' personal health data but not "personal health data [that] is derived solely from other information that is not personal health data, such

242. *Id.*

243. *See id.* at 1 ("This Report focuses on 'mHealth technologies' and 'health social media.'").

244. *See id.* at 29 ("[Non-covered entities] engage in a variety of practices such as online advertising and marketing, commercial uses or sale of individual information, and behavioral tracking practices, all of which indicate information use that is likely broader than what individuals would anticipate.").

245. S. 24, 117th Cong. (2021).

246. *See Klobuchar, Murkowski Introduce Legislation to Protect Consumers' Private Health Data,* AMY KLOBUCHAR MINNESOTA (Feb. 2, 2021) (outlining several key objectives of the Protecting Personal Health Data Act) [perma.cc/Z7EY-A5TF].

247. *Id.*

as Global Positioning System data."[248] This act would apply to femtech apps because they are designed to collect a range of personal health data related to period and fertility tracking. At the same time, Fog Data services would not qualify under this act because health information such as being at a Planned Parenthood is only gathered from non-health data – location data.

This bill also tasks the HHS Secretary to create several uniform policies on consent, third-party marketing, and data retention.[249] The secretary would develop consent standards, considering "the manner in which consent is obtained in a way that uses clear, concise, and well-organized language that is easily accessible, of reasonable length, at an appropriate level of readability, and clearly distinguishable from other matters."[250] The bill would also "limit the transfer of personal health data to third parties and provide consumers with greater control over how their personal health data is used for marketing purposes."[251] Additionally, there would be procedures to allow withdrawal of consent; providing a copy of personal health data; and the right to delete and amend personal health data.[252] If this bill passed in Congress, femtech users would understand the companies' privacy policies better and have more rights regarding the use of their data. Users would have much more control over if and how their personal information is shared with third parties.

While the proposed Protecting Personal Health Data Act would enhance health privacy laws, the bill does not prevent law enforcement from retrieving the protected material.[253] Congress should also enact the proposed Fourth Amendment Is Not for Sale Act to prevent police from evading Fourth Amendment protections and purchasing data from third parties.[254] The bill states law enforcement "may not obtain from a third party in exchange for

248. S. 24. at § 3(1)(C)(i).

249. *See id.* at § 4(a) (listing the HHS Secretary's responsibilities under this act).

250. *Id.* at § 4(b)(3)(B).

251. *Id.* at § 4(b)(3)(C).

252. *Id.* at § 4(b)(3)(E).

253. *See id.* at § 4(b)(2)(D) ("[The Secretary must] consider exceptions to consent requirements under subparagraph (C) for purposes that may include law enforcement, academic research.").

254. The Fourth Amendment Is Not for Sale Act, S. 1265, 117th Cong. (2021).

anything of value a covered customer or subscriber record or any illegitimately obtained information."[255] In other words, this bill would prevent the government from purchasing "covered records" or illegally obtained information from private companies. This government restriction would capture multiple levels of third-party transactions. The act applies whether or not the third party is "the third party that initially obtained or collected" the covered information.[256] Third parties could no longer create a chain of data brokers that evade the Fourth Amendment to sell data to the government. Whether the government seeks to buy health data directly from Flo, its partner ApsFlyer, ApFlyer's data brokers, or eventually from Fog Data, all of these exchanges would be impermissible.

A covered record refers to "a record or other information that (1) pertains to a covered person; (2) and the contents of a communication or location information."[257] Thus, advertising IDs and Fog Data's location services would be covered under this provision. And the act clarifies that the term "pertains" means "information that is linked to the identity of a person" or information "that has been anonymized remove links to the identity of a person; and that, if combined with other information, could be used to identify a person."[258] This clarification prevents third parties from attempting to claim their information is "anonymized," as Fog Data has when in practice the data can easily be tracked back to an individual.

If the government were to violate this bill and purchase a "covered record," any evidence gathered from this exchange "may not be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States."[259] Prohibiting this evidence accomplishes the same outcome as most Fourth Amendment violations: excluding evidence that the government unlawfully obtained from a legal proceeding.

---

255. *Id.* at § 2(2)(A).
256. *Id.* at § 2(2)(B).
257. *Id.* at § 2(1)(C).
258. *Id.* at § 2(1)(J).
259. *Id.* at § 2(4).

Congress should adopt both the proposed Protecting Personal Health Data Act and the proposed Fourth Amendment Is Not for Sale Act. Together, these bills would solve major gaps in Fourth Amendment jurisprudence. The Protecting Personal Health Data Act would extend privacy protections to mobile technologies and social media sites, which HIPAA overlooks. This bill would (1) require femtech apps to clarify and streamline their privacy policies and (2) grant consumers more control over whether femtech apps can share or sell their personal data with third parties. At the same time, the Fourth Amendment Is Not for Sale Act would prevent law enforcement from purchasing covered records, including location data, from private companies. Thus, this bill would break the chain of third parties buying and selling advertising IDs from apps, and police departments could no longer pay for Fog Data's location tracking services.

VII. Conclusion

After the Supreme Court struck down *Roe v. Wade* and states began criminalizing abortion care, women have expressed deep concerns about their personal privacy, especially on period and fertility tracking apps.[260] Police could potentially use a combination of location data and personal health data from femtech apps to prosecute abortions.

Femtech apps store extremely personal data that extends far beyond tracking a woman's last period date.[261] Femtech apps gather personal information such as subscriber information, demographics, and health and wellbeing symptoms.[262] And, often without an individual's knowledge, femtech apps automatically gather data about users' mobile device and location history.[263] Despite the sensitive nature of this information, femtech apps share user data directly with police and with third party

260. *See supra* Part I. (introducing the criminalization of abortions following *Dobbs*).

261. *See supra* Part II. (detailing the personal information that femtech apps store).

262. *See supra* Subpart II.A. (listing examples of information provided by app users).

263. *See supra* Subpart II.B. (explaining types of data that apps automatically collect).

companies.[264] It is particularly concerning when femtech apps sell advertising IDs to third parties because these IDs are "ubiquitous and effective" identifiers in the tracking industry.[265] Fog Data purchases these advertising IDs from apps and then creates a massive, searchable database that they sell to police departments.[266] Police departments can avoid the hassle of filing a court order for a geofence warrant from Google and simply purchase the same location tracking services from Fog Data.[267] Without strong legal protections, these companies will continue to make a profit at the expense of users' privacy.

The Fourth Amendment does not adequately protect the private data femtech apps store and sell to others. The third-party doctrine allows femtech companies to evade Fourth Amendment protections because the government can request their personal data so long as the companies notify users somewhere in their long, convoluted terms of service.[268] There are also no Fourth Amendment restrictions on Fog Data buying personally identifying information from apps and then selling location tracking services to police.[269] Law enforcement can pay a small fee to access Fog Data's billions of location data points and perform geofence searches around any desired area at any time. Thus, the police could perform Fog Data geofence searches around a Planned Parenthood to identify potential suspects for illegal abortions.

To prevent this invasion of privacy, the Supreme Court should extend the principles from *Carpenter* to Fog Data's subscription services. Fog Data captures more location data points than the CSLI technology in *Carpenter*, and it allows police to buy an

264. *See id.* (highlighting how femtech apps share with and sell personal data to third parties).

265. *See* Cyphers, *supra* note 65 (warning of the dangers of advertising IDs).

266. *See id.* (explaining the level of detail that can be attached to an advertising ID).

267. *See* Cyphers & Mackey, *supra* note 89 (describing how police buy location data from Fog Data).

268. *See supra* Subpart IV.A. (applying the third-party doctrine to femtech apps' privacy policies).

269. *See supra* Subpart IV.B. (arguing that Fog Data evades core Fourth Amendment principles).

intimate portrait of someone's life at low cost.[270] The Supreme Court should find, similar to *Carpenter*, that the third-party doctrine does not apply to Fog Data's location-tracking services and that the government must obtain a search warrant before using Fog Data.

Congress should also adopt the proposed Protecting Personal Health Data Act and the proposed Fourth Amendment Is Not For Sale Act to strengthen individual privacy rights. The Protecting Personal Health Data Act would provide more clarity and control to individuals over the third parties buying personal health data from femtech apps.[271] At the same time, the Protecting Personal Health Data Act would prohibit law enforcement from buying location data and other covered records from third parties.[272] The government should not be allowed to evade core Fourth Amendment principles in exchange for money.

The plot of Law & Order episode no longer seems like fiction. The legal landscape in the wake of *Dobbs* poses serious threats to women's privacy and freedom, and law enforcement's surveillance practices may be even more harrowing in real life. It is unsettling to watch as Becca's family hacked into her phone and stalked her all the way from Texas to New York to punish her for seeking an abortion. But what if a stranger working for the government could retrieve your intimate health data—learn about your period cycle, when you last had sex, how many steps you take, your recent miscarriage—and then purchase a record of your daily movements at any point in time. All without any probable cause. Current Fourth Amendment law does not protect women from the profitable data broker industry driving government surveillance. Without judicial or legislative intervention, law enforcement is free begin incorporating Fog Data's services into their investigations of abortion services. Women should be able to decide when to have children with dignity, and without fear of being arrested, investigated, or jailed.

---

270. *See supra* Part V. (proposing a judicial solution to Fog Data's subscription services).

271. Protecting Personal Health Data Act, S. 24, 117th Cong. § 4(b) (2021).

272. The Fourth Amendment Is Not for Sale Act, S. 1265, 117th Cong. § 2 (2021).