DATA AS THE ENEMY OF PRIVACY: EMPLOYING THE FOURTH AMENDMENT TO PROTECT DEVICE DATA IN ABORTION PROSECUTIONS

Hilleary Barbara Gramling*

I. INTRODUCTION[1]

> Like many Americans seeking medical advice, the first obvious step many pregnant people will take to self-manage their abortion will be what they may assume to be a solitary consultation with their personal digital device. Whether this leads them to an online medical or commercial provider of abortion pills, or a network of underground abortion doulas, this initial research that lends a false sense of privacy may leave a detailed data trail for those whose devices later become evidence in an investigation.[2]

The Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization* did more than overturn fifty years of precedent by concluding that the Constitution does not confer the

 Litigation Associate, Phelps Dunbar. J.D., *cum laude*, Stetson University College of Law, 2023; B.A., *summa cum laude*, Emory University, 2017. I would like to offer my thanks and sincere appreciation to my writing advisor Professor Roberta Flowers, for her guidance and direction; to my Articles & Symposia Editor (2023–24) Shelby Ponton, for her thoughtful suggestions, immense dedication, and kind encouragement; to my friend, role model, and Editor in Chief (2023–24) Cameron Kubly, for encouraging me to seek publication; to my mentor, Professor Tomer Stein, for his wisdom, knowledge, and support of the early drafts of this piece; and finally, to my sister, Natalie Gramling, for her role as both my champion and my personal editor. I extend my gratitude to all the Editors and Associates of *Stetson Law Review* who have dutifully shaped and diligently prepared this Article for publication.

1. The landscape around abortion regulation is evolving at a rapid pace. Any references to the number of states with abortion bans, relevant dates, or significant events in this area of law were last updated in December 2023.

2. Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV. 1, 22 (2020) (citing *Many Young Women in the United States Turn to Google for Information on Self-Abortion*, GUTTMACHER INST. (Feb. 26, 2018), https://www.guttmacher.org/news-release/2018/many-young-women-united-states-turn-google-information-self-abortion).

right to abortion.[3] The *Dobbs* decision also represents the first time in American history that the Supreme Court revoked a previously recognized right.[4] More immediately, and of dire consequence,[5] after the Supreme Court relinquished the power to regulate abortion to the states, thirteen states' trigger laws[6] automatically outlawing abortions went into effect.[7] Access to abortions has been eliminated by total bans[8] in fourteen states.[9] In Georgia and South Carolina, abortion is banned after six weeks of pregnancy;[10] Nebraska and North Carolina ban abortion after twelve weeks; Florida and Arizona after fifteen weeks; and Utah after eighteen weeks.[11] In the months since the *Dobbs* decision, a total of twenty-one states ban or mostly ban abortions.[12]

---

3. *See* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2242–48 (2022). The decision opened the door for all other unenumerated rights—rights not explicitly established by the text of the Constitution—to follow suit. *See* Zack Beauchamp, *Could Clarence Thomas's* Dobbs *Concurrence Signal a Future Attack on LGBTQ Rights?*, VOX (June 24, 2022, 2:36 PM), https://www.vox.com/2022/6/24/23181723/roe-v-wade-dobbs-clarence-thomas-concurrence. *Dobbs* is potentially the first domino. *Id.* While overruling these rights (to contraception, same-sex marriage, and same-sex relations) may not happen in the next fifty years, or ever, *Dobbs* has made the revocation of a right possible. *Id.*

4. Dobbs v. Jackson Women's Health Organization, CTR. FOR REPROD. RTS., https://reproductiverights.org/case/scotus-mississippi-abortion-ban/ (last visited Dec. 20, 2023); *see also Dobbs*, 142 S. Ct. at 2242 ("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. . . .").

5. See *infra* pt. II.B. for a discussion of the dire consequences of the Supreme Court returning abortion-regulating power to the states.

6. A "trigger law" is "a currently unenforceable law that upon the occurrence of an event (such as a court decision) becomes enforceable." *Trigger Law*, MERIAM-WEBSTER, https://www.merriam-webster.com/dictionary/trigger%20law (last visited Oct. 30, 2023).

7. Caroline Kitchener et al., *States Where Abortion is Legal, Banned or Under Threat*, WASH. POST (Sept. 18, 2023, 12:32 PM), https://www.washingtonpost.com/politics/2022/06/24/abortion-state-laws-criminalization-roe/; Elizabeth Nash & Isabel Guarnieri, *13 States Have Abortion Trigger Bans—Here's What Happens When* Roe *Is Overturned*, GUTTMACHER INST. (June 6, 2022), https://www.guttmacher.org/article/2022/06/13-states-have-abortion-trigger-bans-heres-what-happens-when-roe-overturned.

8. A "total ban" indicates that abortion is banned with no exceptions for rape or incest. *See* Julie Rovner, *Abortion Bans With No Exceptions May Be Politically Risky*, NPR (June 1, 2022, 11:21 AM), https://www.npr.org/sections/health-shots/2022/06/01/1102364461/abortion-bans-with-no-exceptions-may-be-politically-risky.

9. *Tracking Abortion Bans Across the Country*, N.Y. TIMES (Dec. 8, 2023, 2:30 PM), https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html. These states include Alabama, Arkansas, Idaho, Indiana, Kentucky, Louisiana, Mississippi, Missouri, North Dakota, Oklahoma, South Dakota, Tennessee, Texas, and West Virginia. *Id.*; *see also Is Abortion Still Accessible in My State Now That* Roe v. Wade *Was Overturned?*, PLANNED PARENTHOOD ACTION FUND, https://www.plannedparenthoodaction.org/abortion-access-tool/AL (last visited Oct. 28, 2023).

10. *Tracking Abortion Bans Across the Country*, *supra* note 9.

11. *Id.*

12. *Id.* Some states, including Georgia, South Carolina, Nebraska, North Carolina, Arizona, Florida, and Utah, "mostly ban" abortion by placing "gestational limits" on the

While these bans affect those who are pregnant from seeking accessible abortions, they also foster another consequence—one that has less to do with abortion and everything to do with data.[13] Data from reproductive health apps like period trackers, pregnancy calculators, and Apple Health are extremely valuable to advertisers.[14] Period apps contain a massive amount of personal information—including when individuals could be expecting, whether individuals may have missed their period, and any individuals' self-reported symptoms.[15] This information can be corroborated with data from services like Google, Apple, and Facebook that include individuals' search histories and location-related records.[16] The *Dobbs* decision, in essence, altered the significance and value of this data. The decision transformed phone, device, and app data from tools advertisers use to target their goods and services at specific audiences to "evidence" law enforcement can procure in prosecuting individuals who seek abortions in states where abortions are banned, and reproductive healthcare services are severely restricted.

This transformation, while shocking, is not new—it has been foreshadowed by the use of data in investigations for myriad crimes beyond illegal abortions.[17] For example, in Connecticut, location data was used to charge an individual with murder.[18] In

procedure, allowing abortion up to a certain number of weeks into pregnancy. *Id.* The total list of states that ban or mostly ban abortions is as follows: Alabama, Arizona, Arkansas, Florida, Georgia, Idaho, Indiana, Kentucky, Louisiana, Mississippi, Missouri, Nebraska, North Carolina, North Dakota, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Utah, and West Virginia. *Id.*

13. *See* Karen Tumulty et al., *After the Abortion Ruling, Digital Privacy Is More Important Than Ever*, WASH. POST (July 4, 2022, 7:00 AM), https://www.washingtonpost.com/opinions/2022/07/04/abortion-ruling-digital-privacy-important/.

14. *Id.*

15. Catherine Roberts, *These Period Tracker Apps Say They Put Privacy First. Here's What We Found.*, CONSUMER REPS. (Aug. 30, 2022), https://www.consumerreports.org/health-privacy/period-tracker-apps-privacy-a2278134145/.

16. Kristen Poli, *The Most Popular Period-Tracking Apps, Ranked by Data Privacy*, WIRED (July 20, 2022, 7:00 AM), https://www.wired.com/story/period-tracking-apps-flo-clue-stardust-ranked-data-privacy/.

17. Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.

18. Amanda Watts, *Cops Use Murdered Woman's Fitbit to Charge Her Husband*, CNN (Apr. 26, 2017, 2:58 PM), https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html. In 2015, Richard Dabate described an incident in which a masked intruder broke into his home, tied him up, tortured him, and later shot and killed his wife, Connie, when she returned to the residence. *Id.* However, Dabate himself was ultimately charged with the crime when the police—in aggregating a combination of computer, Facebook, and Fitbit data—discovered that Connie's Fitbit data (which recorded

Arkansas, recordings from an Amazon Echo were sought to potentially corroborate an alleged murder.[19] In Ohio, investigators utilized evidence gleaned from a pacemaker to build a case for arson.[20] In Arizona, Google data collected by police "placed a man's phone near the site of a murder," though he "was later released without charge."[21] Even the cases "against alleged January 6 insurrectionists were built on data the FBI got from Google and social media."[22] And, perhaps, least shocking of all, Immigration and Customs Enforcement bought location data to track the entry points of undocumented immigrants into the United States.[23]

---

a total distance of 1,217 feet that morning) did not match Dabate's original story. *Id.* Her Fitbit should have only recorded a distance of 125 feet if Dabate's account was accurate. *Id.*

19. Eliott C. McLaughlin, *Suspect OKs Amazon to Hand Over Echo Recordings in Murder Case*, CNN BUS. (Apr. 26, 2017, 2:52 PM), https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/. James Bates was arrested on suspicion of first-degree murder in 2017. *Id.* Hoping to gather information regarding how a man came to be found dead in Bates' hot tub, the prosecuting attorney sought recordings from Bates' Amazon Echo smart speaker. *Id.* Bates voluntarily handed over the recordings. *Id.*

20. Amanda Watts, *Pacemaker Could Hold Key in Arson Case*, CNN (Feb. 8, 2017, 1:41 PM), https://www.cnn.com/2017/02/08/us/pacemaker-arson---trnd/. In 2016, Ross Compton's house nearly burnt to the ground. *Id.* Compton informed investigators that he was asleep when the fire began and claimed he packed a few items, climbed out of his bedroom window, and escaped the fire. *Id.* However, the story did not add up for investigators who used his pacemaker—after Compton mentioned his health problems several times—to build the case. *Id.* A cardiologist reviewed the data pulled from the pacemaker and determined that Compton was active during the fire, rather than asleep when he said he was. *Id.*

21. Sara Morrison, *What Police Could Find Out About Your Illegal Abortion*, VOX (June 24, 2022, 12:44 PM), https://www.vox.com/recode/23059057/privacy-abortion-phone-data-roe; *see also* Meg O'Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, PHX. NEW TIMES (Jan. 16, 2020, 9:11 AM), https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374. Police wrongfully arrested Jorge Molina for murder based on location data gleaned from Google and information that a white Honda was at the crime scene. O'Connor, *supra*. While Molina did in fact own a white Honda, he informed the officers that it was often driven without his permission by his stepfather—who had a warrant out in California. *Id.* Molina filed a lawsuit for defamation, gross negligence, and intentional infliction of emotional distress based on the fact that the police investigating the murder knew that the location data often showed Molina in two places at once and that the officers knew he was not the only person to operate the Honda registered to him. *Id.*

22. Morrison, *supra* note 21; Charlie Warzel & Stuart A. Thompson, *They Stormed the Capitol. Their Apps Tracked Them.*, N.Y. TIMES (Feb. 5, 2021), https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html. "Key to bringing the mob to justice has been the event's digital detritus: location data, geotagged photos, facial recognition, surveillance cameras and crowdsourcing." Warzel & Thompson, *supra*.

23. Morrison, *supra* note 21; Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020, 7:30 AM), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600 (detailing the Trump administration's purchase of "access to a commercial database that maps the movements of millions of cellphones in America" to track individuals for use by immigration and border enforcement).

Dobbs' return of abortion-regulating power to the states, absent congressional regulation, fosters a reality where law enforcement will increasingly use data from health-related apps and trackers as evidence to convict individuals who seek or execute illegal abortions[24]—adding a chilling wrinkle to the potential ways in which data can and will be weaponized to prosecute crimes. Even before *Dobbs*, in states where abortion is criminalized, the prosecution of individuals suspected of either purposefully or accidentally terminating their pregnancies was trending upward.[25] These states' vested interest in criminalizing abortion; our unique technological moment in which everyone is "online"; and the prevalence of accessible, minable data from apps, guarantee that digital footprints will be excavated by law enforcement and used by prosecutors—a tactic that may lead to the prosecution of birthing individuals not only for abortions, but for stillbirths and miscarriages.[26]

Indeed, prosecutions for pregnancy termination were occurring pre-*Dobbs*.[27] Between 2006 and 2020, 1,331 individuals were charged or arrested in the United States for actions taken during their pregnancies[28]—an amount three times greater than the total documented during the prior thirty-three years.[29] A report authored by Laura Huss—employed by If/When/How, a

24. *See* Patricia Hurtado & Francesca Maglione, *In a Post-*Roe *World, More Miscarriage and Stillbirth Prosecutions Await Women*, BLOOMBERG (July 5, 2022, 11:30 AM), https://www.bloomberg.com/news/articles/2022-07-05/miscarriage-stillbirth-prosecutions-await-women-post-roe.

25. *Id.* In Nebraska, Celeste Burgess, now nineteen, and her mother, Jessica Burgess, forty-two, were charged just a few weeks after the *Dobbs* decision. This July, Celeste was sentenced to ninety days in jail after pleading guilty "to illegally concealing human remains." The evidence in the case? The Burgesses' Facebook messages. 10/11 NOW & Gray News Staff, *Mother, Daughter Charged After Alleged At-Home Abortion*, 11 NEWS (Aug. 10, 2022, 1:46 AM), https://www.kktv.com/2022/08/10/mother-daughter-charged-after-alleged-at-home-abortion/; Michael Levenson, *Nebraska Teen Who Used Pills to End Pregnancy Gets 90 Days in Jail*, N.Y. TIMES (July 20, 2023), https://www.nytimes.com/2023/07/20/us/celeste-burgess-abortion-pill-nebraska.html.

26. Hurtado & Maglione, *supra* note 24 (detailing "a movement to use state laws on child endangerment, feticide or murder to arrest women whose pregnancies ended" early).

27. *Id.*

28. *Id.* (citing *Arrests and Prosecutions of Pregnant People, 1973–2020*, PREGNANCY JUST. (Sept. 18, 2021), https://www.pregnancyjusticeus.org/arrests-and-prosecutions-of-pregnant-women-1973-2020/).

29. From 1973 to 2005, the number of documented cases of individuals who were charged or arrested for actions taken during their pregnancies was 413. Lynn M. Paltrow & Jeanne Flavin, *Arrests of and Forced Interventions on Pregnant Women in the United States, 1973-2005: Implications for Women's Legal Status and Public Health*, 38 J. HEALTH POL., POL'Y & L. 299, 309 (2018).

legal organization in support of abortion rights—details the number of cases that criminalized self-managed abortion since 2000.[30] Huss "documented 61 cases between the years 2000 and 2020 where people have been criminally investigated or arrested for allegedly self-managing their own abortions or helping someone else do so."[31] Huss explained that "[p]reliminary research from this report found that among data available, the majority of people who were criminalized self-managed exclusively with medication abortion and were living in poverty."[32] Most appalling, Huss highlighted that "[p]eople of color were disproportionately represented when compared to the larger population."[33] Overall, the report documents that "74% of the adult cases involve the criminalization of the person for self-managing their own abortion," contrasted with "26% involv[ing] people helping others self-manage."[34] These kinds of prosecutions will only increase in number as *Dobbs* has ensured the criminalization of abortions in just about half of the country—a reality unseen since the 1970s—and in an era where data is plentiful and poorly protected.[35]

Thus, the Supreme Court, in overruling *Roe v. Wade*[36] and *Planned Parenthood v. Casey*,[37] did more than open the door to the

30. Ari Shapiro et al., *New Report Tracks Criminal Prosecutions of Self-Managed Abortions*, NPR (Aug. 9, 2022, 4:21 PM), https://www.npr.org/2022/08/09/1116590982/new-report-tracks-criminal-prosecutions-of-self-managed-abortions.

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

35. Kashmir Hill, *Deleting Your Period Tracker Won't Protect You*, N.Y. TIMES (June 22, 2023), https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html; Conti-Cook, *supra* note 2, at 3–4 (discussing the case of Latice Fisher, wherein "[h]er statements to nurses, the medical records, and the autopsy records of her fetus were turned over to the local police to investigate whether she intentionally killed her fetus"). For an in-depth description of the facts of Fisher's case, see *infra* pt. II.B.

36. Roe v. Wade, 410 U.S. 113 (1973). Decided in 1973, *Roe* "recognized that the decision whether to continue or end a pregnancy belongs to the individual, not the government." Roe v. Wade, CTR. FOR REPROD. RTS., https://reproductiverights.org/roe-v-wade/ (last visited Sept. 30, 2023). Specifically, *Roe* held that the "guarantee of 'liberty' in the Fourteenth Amendment of the U.S. Constitution, which protects individual privacy, includes the right to abortion prior to fetal viability." *Id.* "For the first time, *Roe* placed reproductive decision-making alongside other fundamental rights, such as freedom of speech and freedom of religion, by conferring it the highest degree of constitutional protection, known as 'strict scrutiny.'" *Id.*

37. Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833 (1992). *Casey*, decided in 1992, marked the Supreme Court's adoption of the "'undue burden' standard for determining the constitutionality of government restrictions on abortion, replacing the strict scrutiny standard adopted in *Roe*." Planned Parenthood v. Casey *(1992): Three Judicial Views on Abortion Restrictions*, CTR. FOR REPROD. RTS. (July 9, 2009),

reexamination of all other unenumerated rights (such as contraception and marriage).[38] The Court arguably created a demand for the prosecution of individuals suspected of terminating their pregnancies in states where abortion is banned.[39] Data from period-tracking apps, search engines, Facebook, Google, Apple, and other sources will become even more valuable for prosecutors who pursue convictions in states where abortions are criminalized.[40] Despite the value of such data, the questions now facing courts and advocates are how and whether this data is protected.[41]

This Article focuses on the privacy concerns that emerge under the U.S. Constitution when personal and device data is sought by law enforcement to prosecute individuals for abortion-related crimes. Before delving into the aforementioned issues, this Article discusses Fourth Amendment protections and the third-party doctrine in the context of *Carpenter v. United States*[42] and its progeny.

The Court has long held the Fourth Amendment does not protect information voluntarily disclosed to others—or third parties—including the data individuals "voluntarily" provide to phone companies, such as call records.[43] However, *Carpenter* established that a person's location information reveals their associations, habits, or beliefs, and, as a result, to procure the data without a warrant is a violation of the Fourth Amendment.[44] Ultimately, this Article concludes that, like *Carpenter*, the

---

https://reproductiverights.org/planned-parenthood-v-casey-1992-three-judicial-views-on-abortion-restrictions/.

38. Beauchamp, *supra* note 3.

39. *See* Hill, *supra* note 35; *see also* Hurtado & Maglione, *supra* note 24. *But see* CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 1 (2022), ("In light of the U.S. Supreme Court's decision in *Dobbs* . . . some Members of Congress and commentators have expressed concerns that law enforcement officials may seek to collect abortion-related personal data for prosecutions in states that have criminalized abortions.").

40. Hill, *supra* note 35; *see also* Conti-Cook, *supra* note 2, at 5 ("This Article presents a sobering forecast; . . . [data] related to . . . reproductive health as evidence of criminal intent will become standard protocol across the country once abortion is again criminalized.").

41. Emilie Smith, *Cycle-Tracking Apps and Data Privacy in the Post-*Roe *Climate*, MARQ. UNIV. L. SCH: FAC. BLOG (Oct. 11, 2022), https://law.marquette.edu/facultyblog/2022/10/cycle-tracking-apps-and-data-privacy-in-the-post-roe-climate/.

42. Carpenter v. United States, 138 S. Ct. 2206 (2018).

43. Elizabeth Goitein, *The Government Can't Seize Your Digital Data. Except by Buying It.*, BRENNAN CTR. FOR JUST. (Apr. 28, 2021), https://www.brennancenter.org/our-work/analysis-opinion/government-cant-seize-your-digital-data-except-buying-it.

44. *Carpenter*, 138 S. Ct. at 2223; *see also* Goitein, *supra* note 43.

collection of device data from search histories or health or period-tracking apps—even when collected from third parties—requires a warrant because this data also reveals a person's associations, habits, or beliefs. Accordingly, this Article argues that mining this data without a warrant constitutes an unreasonable search or seizure, triggering application of the Exclusionary Rule which prohibits use of illegally obtained evidence under the Fourth Amendment.[45]

This Article proceeds in six parts. Part II discusses the history of abortion criminalization and how data has been used as evidence by prosecutors. Part III surveys the history and usage of period-tracking and location-related data. Part IV provides a brief synopsis of the privacy concerns associated with this data under the Fourth Amendment. This Part also discusses application of the Exclusionary Rule, a judicial remedy used to rectify Fourth Amendment violations. Next, Part V describes how courts and advocates should approach using period-tracking and location-related data in criminal prosecutions. Finally, Part VI argues that period-tracking data is protected under the Fourth Amendment by the exception to the third-party doctrine carved out in *Carpenter v. United States.*

Because abortion-related data is widely available,[46] is used by prosecutors to convict individuals for pregnancy termination,[47] and will continue to be used at an increasing rate,[48] this Article asserts that courts should scrutinize the collection of this data. Ultimately, this Article emphasizes that advocates should feel empowered by the protections of the Fourth Amendment to argue that this data is brought within its purview.

45. *See generally* Yale Kamisar, *How We Got the Fourth Amendment Exclusionary Rule and Why We Need It*, 1 CRIM. JUST. ETHICS 4 (1982) (explaining the history and necessity of the exclusionary rule).

46. *See* Shaila Dewan & Sheera Frenkel, *A Mother, a Daughter and an Unusual Abortion Prosecution in Nebraska*, N.Y. TIMES (Aug. 18, 2022), https://www.nytimes.com/2022/08/18/us/abortion-prosecution-nebraska.html.

47. Hurtado & Maglione, *supra* note 24.

48. *Id.*; Katherine Yao & Megan L. Ranney, *Opinion: The Danger of Period-Tracking Apps in a Post-*Roe *World*, CNN (June 16, 2022, 5:51 PM), https://www.cnn.com/2022/06/16/opinions/period-trackers-app-roe-abortion-ranney-yao/index.html.

II. A HISTORICAL SURVEY OF ABORTION CRIMINALIZATION AND USE OF DATA IN PROSECUTIONS

To properly examine the Fourth Amendment's protections and their applicability to period-tracking and location data, a discussion surrounding the history of outlawing abortions is warranted. Also, an investigation of how data has been used in prosecutions of various crimes is beneficial.

A. A Brief History of the Criminalization of Abortions

In May 1972, an apartment building was raided by police where a group known as the "Jane Collective" provided abortions.[49] Abortion "was illegal almost everywhere in the country,"[50] and the Jane Collective, operating out of Chicago, "carried out thousands of abortions from 1969 to 1973."[51] The *Roe v. Wade* decision was not yet instituted, and abortion was a criminal offense in Illinois.[52]

Under strict abortion laws, the Jane Collective facilitated abortion services, via non-medical professionals, to individuals in need.[53] Thus, those assisting individuals with procuring these illegal abortions "may have been the housewife next door, the college student down the block, [or] the local schoolteacher."[54] Those who facilitated abortions were called "Janes," and the tactics of the collective were "worthy of a spy novel."[55] The Janes had a fine-tuned system:

> A woman seeking to end her pregnancy left a message on an answering machine. A "Callback Jane" phoned her, collected information and passed it to a "Big Jane." Patients would be taken first to one address, "the front," for counseling. They were then led, sometimes blindfolded, to another spot, "the place," where a doctor did the abortion.[56]

49. Hill, *supra* note 35.
50. Clyde Haberman, *Code Name Jane: The Women Behind a Covert Abortion Network*, N.Y. TIMES (Oct. 14, 2018), https://www.nytimes.com/2018/10/14/us/illegal-abortion-janes.html.
51. *Id.*
52. Hill, *supra* note 35.
53. Haberman, *supra* note 50.
54. *Id.*
55. *Id.*
56. *Id.*

The rate for an abortion procedure in the 1970s was around $1,000, approximately $6,500 today, but the collective reduced the price to $100 if an individual had insufficient monetary resources.[57]

During the 1972 raid, seven Janes were arrested, some with index cards containing the names and addresses of their patients.[58] The Janes did what they had to: "They didn't know what the police might do with the information, so they got rid of it."[59] The women destroyed the cards in the police van by ripping them up and ingesting them.[60] Ultimately, charges against the Janes were dropped after the Supreme Court issued its ruling in *Roe v. Wade* on January 22, 1973,[61] which concluded that the Fourteenth Amendment's affirmation of liberty rights and protection of individual privacy, imparted to the people through the Ninth Amendment, encompass a right to abortion prior to fetal viability.[62] As a result of abortion's legalization nationwide, the underground network of individuals facilitating abortion access was no longer necessary, and the collective broke apart.[63]

However, apparent in the decades since *Roe* became law, "the political, cultural and religious wars over abortion [did not end]."[64] Before *Dobbs*, *Roe*'s provisions were "steadily chipped away by state laws that ban[ned] . . . [abortions] after a specified number of weeks, or impose[d] mandatory waiting periods, or effectively forbid online purchases of misoprostol and mifepristone," drugs that can facilitate abortions.[65] Pre-*Dobbs*, "[m]ost states require[d] that a licensed doctor prescribe the drugs."[66] Even more strict, many states "insist[ed] that a clinician be physically present when the medications . . . [were] taken, a mandate that . . . [could] create hardship for, say, rural women living far from abortion providers."[67]

57. *Id.*
58. Hill, *supra* note 35.
59. *Id.*
60. *Id.*
61. Haberman, *supra* note 50.
62. Roe v. Wade, 410 U.S. 113, 153 (1973).
63. Haberman, *supra* note 50.
64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.*

B. The Dire Consequences of *Dobbs*

When the Supreme Court decided *Dobbs*, overruling *Roe* and *Casey*, the Court returned the power to regulate abortion to the states, notwithstanding federal regulation, "concluding that the Constitution does not protect the right to an abortion."[68] Revoking federal constitutional protection of abortion, states can now severely limit, restrict, or outright ban abortions.[69] Thirteen states' trigger laws banning abortion in the wake of the overturn of *Roe* and *Casey* went into effect.[70] With abortion regulation relinquished from constitutional protection, barring any legislation by Congress, "[a] third of American women of reproductive age now face excessive travel times to obtain an abortion."[71] The consequences of the connection between abortion bans and travel times are dire:

> In states with total or six-week abortion bans, travel times increased, on average, by more than 4 hours. In Texas, travel time increased from about 15 minutes to an average of eight hours. Researchers estimate that more than 60,000 people who need abortion care will be unable to obtain it if these trends continue.[72]

Abortion is banned from the point of conception in a total of fourteen states, banned at six weeks in two states, and banned at twelve, fifteen, or eighteen weeks in five states.[73] Even when *Roe*'s protections were in place, access to safe, reliable abortions was difficult for many.[74]

Those communities who most struggled to access abortions under *Roe* and *Casey*—particularly people of color, individuals

---

68. Dobbs v. Jackson Women's Health Organization *(2022)*, NAT'L CONST. CTR., https://constitutioncenter.org/the-constitution/supreme-court-case-library/dobbs-v-jackson-womens-health-organization (last visited Nov. 20, 2023); *see also* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2242 (2022).

69. Risa Kaufman, et al., *Global Impacts of* Dobbs v. Jackson Women's Health Organization *and Abortion Regression in the United States*, SEXUAL & REPROD. HEALTH MATTERS, Dec. 2022, at 22, 22.

70. *See id.*

71. Cameron Scott, *Model Shows Where Women Lost Access to Abortion After* Dobbs, U.C. S.F. (Nov. 1, 2022), https://www.ucsf.edu/news/2022/10/424121/model-shows-where-women-lost-access-abortion-after-dobbs.

72. *Id.*

73. *See Tracking Abortion Bans Across the Country*, *supra* note 9 (highlighting different abortion ban lengths among different states).

74. Kaufman, et al., *supra* note 69, at 23.

with disabilities, undocumented individuals, and people living with low incomes or in poverty—now face even greater hardships and "discriminatory obstacles to health care" after the *Dobbs* ruling.[75] For people at the intersection of poverty and minority status, abortion bans are devastating:

> Poverty is deeply intertwined with other forms of structural discrimination, and people of colour, immigrants, LGBTQI + people, people with disabilities, and women and children suffer disproportionately from economic inequalities. With state bans going into effect and clinics shutting down, in many instances people seeking abortion in the United States must now travel across multiple state lines to reach a clinic, which exacerbates the financial and other hardship many already experience. For many, the barriers will simply be too high.[76]

Specifically, about three-fourths of abortions sought in the United States are by individuals who are "poor or have low incomes."[77] State bans and restrictions lead to abortion clinic closures, which not only exacerbates financial hardships and forces those seeking abortion-related care to travel across state lines, but also impacts access to basic reproductive care for services related to fertility, miscarriage, and potential reproductive complications, regardless of an individual's "desired pregnancy outcome."[78]

Finally, the criminalization of abortion now subjects individuals "to criminal prosecution or other punitive legal action because of their pregnancy or an outcome of their pregnancy."[79] These punishments adversely impact people of color, immigrants, and individuals facing poverty.[80] Thus, the status quo has left

75. *Id.* The United States Supreme Court is set to hear a case challenging the Federal Drug Administration's approval of mifepristone, a "two-regimen" abortion drug. Abbie VanSickle, *Supreme Court Will Hear Challenge to Abortion Pill Access*, N.Y. TIMES (Dec. 13, 2023), https://www.nytimes.com/2023/12/13/us/supreme-court-abortion-pill.html?smid=nytcore-ios-share&referringSource=articleShare. The Supreme Court's ruling "could sharply curtail access to the medication, even in states where abortion remains legal"—further restricting an individual's ability to procure a safe, affordable abortion. *Id.*

76. Kaufman, et al., *supra* note 69, at 23.

77. *Id.*; *see also* Hope Sheils, *Overturning* Roe *is a Poverty Issue*, GEO. J. POVERTY L. & POL'Y (Oct. 14, 2022), https://www.law.georgetown.edu/poverty-journal/blog/overturning-roe-is-a-poverty-issue/.

78. Kaufman, et al., *supra* note 69, at 23.

79. *Id.*

80. *Id.*

those who were already struggling to receive necessary reproductive care in the lurch and without access.[81]

C. A Brief History of the Use of Data in Criminal Prosecutions, Generally

Data usage in criminal prosecutions for various crimes sets the stage for data usage in illegal abortion prosecutions. In 1906, in Berkeley, California, the first acknowledged use of data analysis in American policing was initiated by August Vollmer.[82] Vollmer was the University of California Berkeley's first police chief and the founder of the campus' criminology department.[83] Vollmer organized patrol beats based on police report reviews and by mapping crimes.[84] Since then, law enforcement has developed a vested interest in data use for the conviction and prosecution of individuals.[85] With the availability of constant digital trails in the age of modern technology, incriminating data about a decision to end a pregnancy is harder to hide and easier to find.[86]

Pre-*Dobbs*, data—such as search history or abortion clinic website visits—was used to criminalize individuals for abortion-related crimes.[87] In 2017, Latice Fisher, a Mississippi woman, was charged with second-degree murder after a stillbirth she delivered in her home.[88] In the evening of April 27, 2017, Fisher, a Black woman with three children, "had an upset stomach at her home in Starksville, Mississippi."[89] Fisher then "went to the bathroom to have a bowel movement, [or so] she thought."[90] Next, the

81. *See id.*

82. Amy Vracar, *The Evolution of Law Enforcement Data*, BENCHMARK ANALYTICS (Apr. 27, 2020), https://www.benchmarkanalytics.com/blog/the-evolution-of-law-enforcement-data/.

83. Gretchen Kell, *August Vollmer Biography Explores Famous Police Chief's UC Berkeley Ties*, BERKELEY NEWS (Apr. 19, 2017), https://news.berkeley.edu/2017/04/19/august-vollmer-biography-explores-famous-police-chiefs-uc-berkeley-ties/.

84. Vracar, *supra* note 82.

85. *See How Is Data Collection Used in the Justice System?*, MEDIUM: OPEN DATA SCI. (Apr. 26, 2022), https://odsc.medium.com/how-is-data-collection-used-in-the-justice-system-277138d8edfd.

86. *See, e.g.*, Hill, *supra* note 35 (discussing how data from period-tracking apps can be used to monitor possible abortions).

87. *See id.*

88. *Id.*

89. Lauren Rankin, *How an Online Search for Abortion Pills Landed this Woman in Jail*, FAST CO. (Feb. 26, 2020), https://www.fastcompany.com/90468030/how-an-online-search-for-abortion-pills-landed-this-woman-in-jail.

90. *Id.*

unexpected happened: "Instead, she reportedly gave birth to what her lawyers say was a stillborn baby."[91] Later that night, her husband dialed 911, EMTs rushed to her home, and the fetus was pronounced dead at OCH Regional Medical Center.[92]

Prosecutors asked "whether or not Latice Fisher gave birth to a stillborn or a living baby," and wondered "[d]id Fisher have a tragic accident or was she a neglectful murderer?"[93] To answer that question, a state medical examiner used "a 'lung flotation' test,[94] a controversial and unreliable method likely developed in the 1600s," to conclude that the fetus was born alive.[95] However, this conclusion did not provide prosecutors with a motive for Fisher.[96] For that, investigators downloaded the contents of Fisher's phone—including her internet search history.[97] She admitted to searching the internet for how to induce a miscarriage.[98] The state's evidence indicated "that in her third trimester, Ms. Fisher 'conduct[ed] internet searches, including how to induce a miscarriage, "buy abortion pills, mifepristone online, misoprostol online," and "buy misoprostol abortion pill online,"' and [that she] purchased misoprostol online."[99] Introducing no physical evidence that the fetus was alive at birth or that an abortion had occurred, the state leaned almost exclusively on Fisher's cell phone data:

---

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.* The test is conducted by placing a baby's lung in water. *Id.* Utilized in El Salvador "where it is completely illegal to terminate one's pregnancy," the test was "used by Salvadoran courts to convict dozens of women of infanticide over the last two decades." Kathy Bougher, *Report: 'Scientific' Test Used to Convict Women in El Salvador Is Anything But*, REWIRE NEWS GRP. (Oct. 17, 2014, 5:29 PM), https://rewirenewsgroup.com/2014/10/17/report-scientific-test-used-convict-women-el-salvador-anything/. In a 2014 interview about abortion on *Frente a Frente*, a right-wing national television talk show, Dr. José Miguel Fortin Magaña, "the director of the Salvadoran Institute for Legal [Forensic] Medicine, which reports to the Supreme Court," explained the mechanisms of the test. *Id.* As part of the autopsy, the lungs are removed from the fetus and put in a container of liquid. *Id.* If the lungs float, the baby is concluded to have been alive—when the baby is in the womb it has not yet breathed air and only lungs that have breathed air will float. *Id.* If the lungs sink to the bottom of the container, then the baby is concluded to have never taken a breath. *Id.*

95. Rankin, *supra* note 89.

96. *See id.*

97. Hill, *supra* note 35.

98. *Id.*

99. Conti-Cook, *supra* note 2, at 49 (quoting Ryan Phillips, *Infant Death Case Heading Back to Grand Jury,* STARKVILLE DAILY NEWS (May 8, 2019), https://www.starkvilledailynews.com/infant-death-case-heading-back-to-grand-jury/article_cf99bcb0-71cc-11e9-963a-eb5dc5052c92.html).

> Without the information in her phone, it seemed clear that the State would have insufficient evidence to sustain a prosecution. Her digital data gave prosecutors a "window into [her] soul" to substantiate their general theory that she did not want the fetus to survive even if the abortion medication she pursued would have been unable to terminate her pregnancy in the third trimester.[100]

Likewise in Indiana, text messages sent to a friend about taking abortion pills late in a pregnancy were used to convict a woman of feticide and neglect of a dependent.[101] Purvi Patel, a thirty-two-year-old woman, texted her friend in April 2013 "about an irregular menstrual cycle and cramping."[102] The friend advised Patel to seek out a doctor, but Patel did not.[103] The texts continued from May through June, when Patel took a pregnancy test—the result was positive.[104] This compelled Patel to "text message[] her friend about ordering abortion pills from an 'international pharmacy,' and when the friend asked Patel three more times to see a doctor, she [Patel] replied, 'I'd rather not even go to a doc. I just want to get this over with.'"[105] According to the remaining text messages, the pills arrived in early July, but Patel did not take them until July 10, and "continu[ed] to provide a detailed account of her situation to her friend."[106] On July 13, Patel texted her friend, "Just lost the baby."[107] While Patel ultimately told her nurses she "wrapp[ed] the baby in plastic bags and put[] it in a dumpster behind a Target store,"[108] the texts still played a crucial role in Patel's criminal trial—they provided motive.[109] "Patel

100. *Id.* (quoting C.M "Mike" Adams, *Digital Forensics: Window into the Soul,* FORENSIC (June 10, 2019), https://www.forensicmag.com/518341-Digital-Forensics-Window-Into-the-Soul/).

101. Hill, *supra* note 35.

102. Kelli Stopczynski, *Prosecutors: Text Messages Detail Weeks Leading Up to Patel's Forced Abortion*, WSBT 22 (Apr. 2, 2015, 9:38 PM), https://wsbt.com/news/local/prosecutors-text-messages-detail-weeks-leading-up-to-patels-forced-abortion.

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.*

107. *Id.*

108. *Id.*

109. *See* Amanda Gray, *Texts, Autopsy Results Shown in Patel Trial*, S. BEND TRIB. (Jan. 29, 2015, 5:00 AM), https://www.southbendtribune.com/story/news/local/2015/01/29/exts-autopsy-results-shown-in-patel-trial/46229893/; Jill Disis, *The Case of Purvi Patel: Should a Pregnant Woman Be Charged with Feticide?*, INDYSTAR (May 3, 2015, 8:20 AM), https://www.indystar.com/story/news/crime/2015/05/03/case-purvi-patel-pregnant-woman-charged-feticide/26825871/.

became the first Indiana woman to be convicted of feticide in connection with her own miscarriage."[110]

Patel and Fisher's cases both occurred pre-*Dobbs* and foreshadow the role data can play in illegal abortion prosecutions even when constitutional protection of an individual's right to procure the procedure was steadfastly in place. With this protection largely returned to the states, data has become even more valuable to prosecutors—creating an incentive for them to obtain it. Information about where individuals go, collected on their devices, is already being sold by data brokers—including information that can show an individual went to an abortion clinic.[111] There are multiple exposés outlining the depth of information revealed from data:

> When The New York Times investigated the supposedly anonymized data on the market in 2018, it was able to identify a woman who had spent an hour at a Planned Parenthood in Newark. In May, a journalist at Vice was able to buy information from a data broker about phones that had been carried to Planned Parenthoods over the course of a week for just $160.[112]

Beyond easily obtainable geolocation data, high school aged individuals with periods are being targeted to provide period-related information to their schools.[113] In Florida, questions about high school athletes' menstrual cycles and history were added to a required health form for participation in high school athletics.[114] While the Florida High School Athletic Association's board of directors voted fourteen to two to remove the questions, the form's controversy highlights how fraught the implications of the collection of personal health data have become.[115]

Unlike 1972, where individuals could rip up the information they had and ingest it, digital footprints are "regularly sold by data

110. Disis, *supra* note 109.
111. Hill, *supra* note 35.
112. *Id.*
113. *See* Sarah McCammon, *Florida High School Athletes Won't Have to Report Their Periods After Emergency Vote*, NPR (Feb. 9, 2023, 5:28 PM), https://www.npr.org/2023/02/09/1155731808/plan-to-collect-menstrual-data-on-high-school-athletes-in-florida-is-voted-down.
114. *Id.*
115. *See id.*

brokers";[116] available for seemingly anyone to find;[117] and can show location,[118] an irregular period,[119] an individual's search history,[120] and even an individual's conversations.[121] Also, unlike 1972, what law enforcement will do with the information gleaned from devices is clear: child bearers can and will be prosecuted.[122] Because *Dobbs* returned nearly unfettered abortion regulation power to the states, and twenty-one of those states ban or seriously constrain abortion, more than half the country is ripe for zealous enforcement of anti-abortion laws.[123] Law enforcement did not have device data in 1972, but they do now.[124] Thus, two relevant inquiries remain: whether this kind of data mining is legal under the Fourth Amendment, and whether it is admissible in court.

III. PERIOD AND LOCATION-TRACKING

Social media "is one of the most popular online activities,"[125] with "over 4.59 billion people . . . using social media worldwide" in 2022.[126] Most people using social media think of it as an amplifier for their inner thoughts, and feel comfortable enough to share "woes, ups and downs," and even "a few strong opinions on different matters."[127] Some people share these feelings and views publicly, others in private chat threads, but regardless of the chosen venue, one lesson is apparent: individuals "should clearly understand the consequences" of sharing their opinions online.[128] Messages or texts sent in the heat of the moment, such as rants

116. Hill, *supra* note 35.
117. *See id.*
118. *Id.*
119. *See, e.g.*, Disis, *supra* note 109.
120. *See* Conti-Cook, *supra* note 2, at 49.
121. *See* Disis, *supra* note 109.
122. *See* Shefali Luthra, *Abortion Bans Don't Prosecute Pregnant People. That May Be About to Change.*, THE 19TH (Jan. 13, 2023, 1:05 PM), https://19thnews.org/2023/01/abortion-bans-pregnant-people-prosecution/ (describing legislation in Oklahoma and statements from the Alabama attorney general that "could foreshadow new efforts to punish people who induce their own abortions").
123. *See* Kitchener et al., *supra* note 7.
124. *See* Hill, *supra* note 35.
125. Stacy Jo Dixon, *Number of Social Media Users Worldwide from 2017 to 2027*, STATISTA (Aug. 29, 2023), https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.
126. *Id.*
127. Andrew Arnold, *Here's How Social Media Can Be Used Against You in Court*, FORBES (Dec. 30, 2018, 4:57 AM), https://www.forbes.com/sites/andrewarnold/2018/12/30/heres-how-social-media-can-be-used-against-you-in-court/?sh=2d3e192e6344.
128. *Id.*

about a spouse or boss, may reappear in litigation.[129] Consequently, people should be aware of this possibility before sending digital messages. Courts often admit content and posts from social media as evidence[130] and, "[c]ontrary to popular belief, it is legal to use communications garnered from social media sites as evidence" in court.[131] But what about communications and information from other kinds of apps?

Millions of people utilize apps to assist them in tracking and monitoring their menstrual cycles.[132] Flo, which dubbed itself "the most popular period and cycle tracking app," has forty-three million active users.[133] Clue, another period-tracking app, follows with twelve million active users.[134] Period and cycle-tracking apps store the personal health data of their users, and some of the "most intimate" data an individual can provide—specific and numerous details about menstruation and pregnancy.[135] Data from these apps could be "subpoenaed or sold to a third party" and "used to suggest that someone has had or is considering an abortion."[136]

However, period-tracking data is not the only means of utilizing technology to link an individual to obtaining an abortion.[137] "If someone is sitting in the waiting room of a clinic that offers abortion services and is playing a game on their phone, that app might be collecting location data."[138] Datasets can be purchased for nefarious purposes, and this is troubling when search histories and location data related to abortion information or services can identify an individual.[139] Even more terrifying, this information is not difficult to obtain—by individuals or law enforcement.[140] Records of search histories and location-related data "offer a way for private citizens to report another person for seeking an abortion."[141] Widely used apps have corporate

129. *Id.*
130. *Id.*
131. *Id.*
132. Rina Torchinsky, *How Period Tracking Apps and Data Privacy Fit into a Post*-Roe v. Wade *Climate*, NPR (June 24, 2022, 3:06 PM), https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps.
133. *Id.*
134. *Id.*
135. *See id.*
136. *Id.*
137. *Id.*
138. *Id.*
139. *Id.*
140. Hill, *supra* note 35.
141. Torchinsky, *supra* note 132.

decisionmakers, and their cooperation with law enforcement during criminal investigations is not uncommon—though it is historically related to child pornography or "exploitative imagery."[142] Experts opine that where abortion is criminalized, "period-tracking data could become a target for investigators."[143]

Unfortunately, and critical to the prosecutions of illegal abortions, the degree to which period-tracking data is actually private for the user can be unclear.[144] In 2021, the Federal Trade Commission ("FTC") reached a settlement with Flo regarding "allegations that it misled users about the disclosure of their personal health data."[145] Following a *Wall Street Journal* investigation in 2019 illuminating that "the app informed Facebook when a user was having their period or if they [the user] informed the app that they intended to get pregnant," the FTC mandated that "Flo must undergo an independent review of its privacy policy and obtain user permissions before sharing personal health information."[146]

Regardless of a given app's privacy policies, the data input by an individual using said "app could reach far beyond the phone or the app" being used—"data could actually be all over the network at this point."[147] Whether this data is "safe" for users to continue logging is largely dependent on where they are located and what that individual state's laws are.[148] Nevertheless, the breadth and easy accessibility of this data could incentivize law enforcement to seek it out when prosecuting illegal abortions.[149] For example, "[i]f police are interested in data stored on a user's device, they would need a warrant," however, "if the data is in the cloud and owned by a company," law enforcement could obtain it via subpoena, which has a lower legal bar than a warrant.[150] The myriad types of personal data from health and financial records, to location data and electronic communications, to data from period-tracking apps "might shed light on an individual's abortion decision, and law enforcement could seek such information, either directly from the

142. *Id.*
143. *Id.*
144. *Id.*
145. *Id.*
146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.*
150. *Id.*

entity collecting the data or from another entity to whom the data has been shared or sold."[151] The bottom line, according to Andrea Ford, a research fellow at the University of Edinburgh, is that "the most secure option might just be the most old-fashioned: tracking your cycle on paper. 'If you want to be safe, use a paper calendar.'"[152]

IV. PRIVACY CONCERNS AND THE FOURTH AMENDMENT

Despite *Dobbs*' relinquishment of abortion regulating power to the states, absent legislation from Congress, "[f]ederal law may affect law enforcement's ability to collect [data]."[153] Beyond the Fourth Amendment, data related to healthcare, finances, electronic communications, and other personal information may be protected from disclosure by federal privacy statutes.[154] However, "[m]any entities not subject to these specific federal privacy statutes may still collect, directly or indirectly, data relevant to an individual's abortion decision, such as their geolocation data or web browsing activity."[155] Further, because "[c]urrent[] privacy laws are a cluttered mess of different sectoral rules,"[156] this Article is limited to a discussion of how the protections of the Fourth Amendment do and should apply to period-tracking and location data related to abortion prosecutions.

Indeed, data collection organizations must comply with the FTC regulations of "unfair or deceptive acts or practices."[157] Further, in the wake of *Dobbs*, President Biden issued an Executive Order seeking to shield abortion-related information and data by "prompt[ing] the Department of Health and Human

151. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 1 (2022); *see* Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022, 12:46 PM), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood (describing how SafeGraph, a company that obtains location data from apps installed on individual's phones, sold a week's worth of location data of more than 600 Planned Parenthood locations for just $160).

152. Torchinsky, *supra* note 132.

153. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 1 (2022).

154. *Id.*

155. *Id.*

156. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

157. 15 U.S.C. § 45.

Services (HHS) and the . . . FTC to use their statutory authorities to protect this data."[158] However, discussion of federal privacy laws, President Biden's Executive Order, and the application of these items to such data is appropriate for another Article and requires significant conversation that rests outside this Article's scope.

A. The Fourth Amendment

The Fourth Amendment to the United States Constitution reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[159]

This Amendment "prohibits federal and state officials from conducting 'unreasonable searches and seizures,'"[160] and "generally requires law enforcement officials to obtain a warrant before collecting personal data, although this requirement typically does not apply when the information is held by a third party."[161]

For abortion prosecutions, the key inquiry is whether data collected from an app on an individual's phone falls within the Fourth Amendment's protections. For this to be true, the question comes down to how the location of that data is viewed. Is the collection of period and health-related data considered to be a search of the individual? Or, because that data is housed in apps and on an individual's electronic devices, is that data considered to be "held by a third party" and thus not protected by the Fourth Amendment?

158. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 1 (2022).

159. U.S. CONST. amend. IV.

160. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 1 (2022) (quoting U.S. CONST. amend. IV).

161. *Id.*

1. The Individual

If a law enforcement "official violates an individual's reasonable expectation of privacy," a "search" or "seizure" may be unreasonable, even without physical intrusion, under Supreme Court caselaw.[162] For a search to be considered reasonable, an official must provide probable cause to support a warrant from a court.[163] Without a warrant, a search or seizure may only be conducted under limited circumstances (for example when the search is incident to an arrest).[164] Additionally, the Fourth Amendment only protects those areas, spaces, or items in which an individual is deemed to have a "reasonable expectation of privacy."[165] Without this reasonable expectation of privacy, the protections of the Fourth Amendment do not apply.[166]

The inquiry for whether an individual has a reasonable expectation of privacy is piloted by several Supreme Court cases.[167] As held by *Katz v. United States*, the Supreme Court case that provides the test for determining whether a reasonable expectation of privacy exists, "the Fourth Amendment protects people, not places."[168] The dispositive question is whether an individual has a reasonable expectation of privacy in that specific location, not whether a certain location is private in theory.[169] Thus, "a privacy interest, in the constitutional sense, consists of a reasonable

---

162. *Id. See generally* Katz v. United States, 389 U.S. 347, 357 (1967) (finding that law enforcement searches without judicial approval are unreasonable under the Fourth Amendment).

163. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 1 (2022); *see also* New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) (explaining that determining the reasonability of a search requires a balancing test between how intrusive the search is and the necessity of the search).

164. *See What Does the Fourth Amendment Mean?*, U.S. CTS., https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0 (last visited Nov. 1, 2023).

165. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 1 (2022); *see also T.L.O.*, 469 U.S. at 337.

166. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 1 (2022); *see also* Smith v. Maryland, 442 U.S. 735, 743–45 (1979).

167. *See* CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 1 (2022).

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

169. Marcia Shein, *The Fourth Amendment and the Exclusionary Rule*, SHEIN, BRANDENBURG & SCHROPE FED. CRIM. L. CTR. (Aug. 2, 2018), https://federalcriminallawcenter.com/2018/08/the-fourth-amendment-and-the-exclusionary-rule/ (citing Rakas v. Illinois, 439 U.S. 128, 139–43 (1978)).

expectation that uninvited and unauthorized persons will not intrude into a particular area."[170] Accordingly, an individual maintains a reasonable expectation of privacy in a given place even in scenarios where she freely admits guests or where she has an obligation to allow certain people entrance.[171] Her "expectation of privacy" encompasses the belief that those who are uninvited "will not intrude in a particular way."[172] Additionally, she maintains certain rights despite waiving others. For example, while a person in a public place may have waived her right not to be seen, the mere fact that she is in public does not mean she has given up her right to a private conversation.[173]

2. The Third Party

However, this protection "seldom appl[ies]" when the information is sought from a third party.[174] The Supreme Court has held that when law enforcement officials request an individual's records from a bank[175] or attempt to obtain phone records from a provider or carrier,[176] the protections of the Fourth Amendment do not apply.[177] Dubbed the third-party doctrine, the Court reasoned that an individual who voluntarily shares their personal information with a third party loses Fourth Amendment protections because that person no longer maintains "a reasonable expectation of privacy" in the shared information.[178] Within the context of collecting data from period-tracking apps for use in illegal abortion prosecutions, the Fourth Amendment's protections may or may not be implicated depending on where exactly information is stored and collected from.[179] Initially, it would seem that when an individual has shared their personal health data

170. *Id.*
171. *Id.* (citing Stoner v. California, 376 U.S. 483, 489–90 (1964)).
172. *Id.*
173. *Id.* (citing *Katz*, 389 U.S. at 352).
174. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 2 (2022).
175. *See* United States v. Miller, 425 U.S. 435, 440–45 (1976).
176. *See generally* Smith v. Maryland, 442 U.S. 735 (1979) (stating there is no reasonable expectation to privacy regarding the phone numbers an individual dials).
177. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 2 (2022).
178. *Id.*
179. *Id.* at 1–2.

with a period-tracking app, that information would, as it is held by a third party, not be protected by the Fourth Amendment.[180]

3. Carpenter v. United States

However, in *Carpenter v. United States* the Supreme Court acknowledged a third-party doctrine limitation when law enforcement officials sought and obtained "a large volume of customers' historical cell-site location information (CSLI) from cell phone providers, which showed the suspect's detailed movements over . . . 127 days."[181] While a third party phone provider maintained this information, the Court held that Fourth Amendment protections applied because the data was "a necessary byproduct of consumers' cell phone usage, which itself is 'indispensable to participation in modern society.'"[182] Thus, the location data was more akin to information obtained directly from an individual (in which the individual maintains a reasonable expectation of privacy), rather than information obtained from a third party (in which the individual does not have a reasonable expectation of privacy in information voluntarily shared).[183] The Court reasoned that "a world of difference" existed between the bank records recognized in its prior third party cases[184] and the CSLI in *Carpenter*, because the CSLI reveals the physical location of an individual "every day, every moment" over an extended period.[185] The *Carpenter* decision followed a prior throughline of caselaw addressing an individual's "reasonable expectation of privacy in their physical location and movements," with the Court's majority finding that "the Fourth Amendment would protect against law enforcement surreptitiously using GPS tracking to conduct extended and comprehensive surveillance of a person's movements."[186]

---

180. *Id.* at 2.

181. *Id.* (citing Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018)).

182. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2220).

183. *Id.*

184. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2219). *See generally* United States v. Miller, 425 U.S. 435 (1976) (finding when a bank customer reveals their account information to the bank that customer assumes the risk that the bank can convey that information to the government).

185. *Carpenter*, 138 S. Ct. at 2220.

186. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 2 (2022); *see also* United States v. Jones, 565 U.S. 400, 404–06 (2012) (determining the use of a GPS device installed by law

4. Interpreting Carpenter *to Protect Period-Tracking Data*

Thus, the Fourth Amendment's protections against unreasonable searches and seizures apply in the abortion context in two situations: (1) where law enforcement seeks to collect information directly from an individual and that individual is found to have a reasonable expectation of privacy in that information, and (2) where law enforcement seeks to collect data from a third party, and the nature of that data is so factually similar to *Carpenter* that it is brought within the ambit of the Fourth Amendment's protections.[187] Regarding the former, law enforcement officials would need to procure a warrant in order to collect and search an individual's cell phone or other devices to review texts, location data, app usage, or other device-related evidence to investigate an individual's abortion decision.[188] The rub, so to speak, is with the latter situation, and whether the Fourth Amendment protects against the collection of abortion-related data or records from a third party, such as a healthcare provider, financial establishment, or data broker.[189]

Regarding the collection of information provided by individuals to third parties, caselaw is lacking—advocates must draw firm comparisons between collected data and the facts of *Carpenter*.[190] If drawn successfully, a court could find the third-party doctrine does not apply, bringing data under the Fourth Amendment's protections, when three facts exist: (1) the data sold by data brokers is "exhaustive location information from a third party that tracks an individual's movements over a long period of time"; (2) the data was "gathered by virtue of the individual's use of a technology that has been deemed essential to participation in modern society"; and (3) the "technology does not meaningfully permit the consumer to opt out of the collection and storage of the relevant data."[191]

---

enforcement in a person's vehicle constitutes a search within the protections of the Fourth Amendment); United States v. Knotts, 460 U.S. 276, 283–84 (1983) (dictum) (reasoning comprehensive surveillance of a person, such as twenty-four-hour surveillance, could implicate Fourth Amendment issues).

187. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 2 (2022).

188. *Id.*

189. *Id.*

190. *Id.*; Conti-Cook, *supra* note 2, at 45.

191. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 2 (2022).

Because nearly "50 million . . . [individuals] worldwide use period tracker apps"[192] on smart and cellular phones, and the Supreme Court deemed cellular phone usage "indispensable to participation in modern society,"[193] this Article argues data stemming from an individual's period-tracking app is factually similar to *Carpenter*, and thus should be protected by the Fourth Amendment. Because "[c]ourts' application of *Carpenter* to other digital data, like search engine queries, purchasing history, and health data from wearable devices, is still developing,"[194] advocates must draw these similarities for courts as these cases arise.

Accordingly, advocates should emphasize that the "private, sensitive, and confidential" nature of the data stored on cellular and smart phones, or other devices, is considered private by society and thus any data sought from a cellular or smart phone, or other device, has been involuntarily given to a third party.[195] Advocates must be prepared to stress that collection of data from a third party (such as a healthcare provider) does, indeed, constitute a "search" under the third-party doctrine. The information sought, similar to CSLI in *Carpenter*, can reveal an individual's location at any given moment, as well as—in the case of period trackers—their intimate thoughts about their bodies and their healthcare choices.[196]

The American Civil Liberties Union ("ACLU") put it quite succinctly in its Amicus Curiae Brief in Support of Respondent-Appellant in *United States Department of Justice v. Ricco Jonas*, arguing that the Drug Enforcement Administration, in the course of a criminal investigation, by obtaining an administrative subpoena, unlawfully pursued patient information maintained by "a prescription drug database."[197] The ACLU argued that "the decision to visit a physician and pharmacist to obtain necessary medical care is not in any meaningful sense voluntary."[198] This principle should extend to virtual circumstances: "If a person is seeking online reproductive health advice because they have few

192. Lauren Worsfold et al., *Period Tracker Applications: What Menstrual Cycle Information Are They Giving Women?*, WOMEN'S HEALTH, Oct. 9, 2021, at 1, 1.

193. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

194. Conti-Cook, *supra* note 2, at 40.

195. *Id.* at 45.

196. *See id.* at 48.

197. *Id.* at 44–45.

198. Brief for American Civil Liberties Union et al. as Amici Curiae in Support of Respondent-Appellant at 6, U.S. Dep't of Just. v. Ricco Jonas, 24 F.4th 718 (1st Cir. 2022) (No. 19-1243).

local alternatives, then perhaps one could argue that virtual medicine was one's only alternative and that 'there is no way to avoid leaving behind a trail of [medical] data.'"[199]

Privacy advocates can, and should, similarly argue that an individual—who has few helpful alternatives and who seeks online or app-related reproductive or abortion-related advice and care—had no choice but to do so; therefore, their personal health data was involuntarily provided to third parties.[200] In fact, the simply reality for many individuals who seek abortion-related care as one of their only means of obtaining health-related information is to turn to apps and the internet.[201] Alternative options are foreclosed when clinics are mandated to stop providing abortion-related care,[202] abortions are increasingly criminalized nationwide,[203] and necessary clinics, doctors, and drugs are inaccessible.[204] In a post-*Dobbs* world, advocating for the protection of period-tracking data under the Fourth Amendment is essential. This advocacy is urgent when the law is unclear, and when law enforcement is seeking abortion-related data "to build cases to prosecute . . . [individuals] seeking abortions or abortion-inducing medication."[205]

199. Conti-Cook, *supra* note 2, at 45 (alteration in original) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018)).

200. *Id.*

201. *Id.* at 22, 24.

202. Marielle Kirstein et al., *100 Days Post-*Roe*: At Least 66 Clinics Across 15 US States Have Stopped Offering Abortion Care*, GUTTMACHER INST. (Oct. 6, 2022), https://www.guttmacher.org/2022/10/100-days-post-roe-least-66-clinics-across-15-us-states-have-stopped-offering-abortion-care (describing how in the 100 days since *Roe v. Wade* was overturned 66 clinics across 15 states "have been forced to stop offering abortions").

203. Katrina Kimport, *Here's What We Can Expect Post-*Dobbs*, According to Research*, U.C. S.F.: ADVANCING NEW STANDARDS IN REPROD. HEALTH (Sept. 7, 2022), https://www.ansirh.org/research/research/heres-what-we-can-expect-post-dobbs-according-research ("Based on published research, three effects of the *Dobbs* decision are predicted: more people surveilled and criminalized for activities during pregnancy; more people denied abortion care; and more delays in obtaining abortion care.") (emphasis added).

204. Conti-Cook, *supra* note 2, at 24, 29 (stating "that the majority of Americans from a wide-range of demographic backgrounds own a smartphone" and that "[p]regnant people are also seeking medical advice online at increasing rates").

205. Katherine Tangalakis-Lippert, *Police Are Prosecuting Abortion Seekers Using Their Digital Data—And Facebook and Google Help Them Do It*, BUS. INSIDER (Mar. 4, 2023, 10:08 PM), https://www.businessinsider.com/police-getting-help-social-media-to-prosecute-people-seeking-abortions-2023-2.

B. The Exclusionary Rule

While the Exclusionary Rule is not an additional protection—as it only applies if the Fourth Amendment was violated[206]—the rule must be discussed as a means of rectifying situations in which period-tracking data was obtained as the result of an illegal search or seizure. A judicially crafted remedy, the Exclusionary Rule aims to reduce misconduct by law enforcement by curing the use of illegally obtained evidence.[207]

If evidence is gathered during an *illegal* search or seizure, violating the Fourth Amendment, the Exclusionary Rule disallows the use of that evidence against the victim of that illegal search or seizure in a criminal proceeding.[208] Evidence obtained in violation of the Fourth Amendment also includes subsequent evidence discovered as a result of the violation, "the 'fruit' of such illegal conduct."[209] This Article argues that because so many individuals depend and rely on their cellular and smart phones and devices[210]—while access to abortion-related care continues to be restricted nationwide—[211]and a significant number of individuals use period-tracking apps to monitor their reproductive health,[212] this data reveals personal information comparable to the CSLI used in *Carpenter*. Therefore, obtaining any data from a period-tracking app without a warrant is a violation of the Fourth Amendment—and a product of an illegal search or seizure—regardless of the source, individual or a third party.

Additionally, "search or web browsing history," including period-tracking data, "obtained either through the device or from the search engine should also be protected under *Carpenter* because 'the deeply revealing nature of [the data]' and 'its depth, breadth, and comprehensive reach . . . does not make it any less deserving of Fourth Amendment protection.'"[213] Unfortunately, the status quo, and the Supreme Court's protection of bank and phone

206. Shein, *supra* note 169.
207. *Id.*
208. *Id.* (citing Mapp v. Ohio, 367 U.S. 643, 654 (1961)).
209. *Id.* (quoting Wong Sun v. United States, 371 U.S. 471, 488 (1963)).
210. Conti-Cook, *supra* note 2, at 29.
211. *See Tracking Abortion Bans Across the Country*, *supra* note 9; Haberman, *supra* note 50.
212. Torchinsky, *supra* note 132.
213. Conti-Cook, *supra* note 2, at 43 (alteration in original) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018)).

records from collection by law enforcement without a warrant "fail[] to accommodate new, 'distinct categor[ies] of information' born from 'the seismic shifts in digital technology'" such as "[t]racking cookies, like historical CSLI."[214] However, with period-tracking data brought into the ambit of *Carpenter*, making its obtainment without a warrant an illegal search, the Exclusionary Rule renders any evidence discovered as a result of obtaining that data inadmissible, regardless of its procurement from an individual or a third party.

To acquire period-tracking data would be in violation of *Carpenter* and its progeny, a violation of the Fourth Amendment, and would constitute an illegal search. As a result, any information gleaned from said "search," (i.e., the search of the contents of a phone), would be considered inadmissible evidence—the "fruit of the poisonous tree"[215] of an illegal search. In essence, this doctrine, the "fruit of the poisonous tree," expands the Exclusionary Rule further to find "evidence inadmissible in court if it was derived from evidence that was illegally obtained."[216] Extending the Exclusionary Rule, "the metaphor suggests, if the evidential 'tree' is tainted, so is its 'fruit.'"[217] Thus, with device data brought under *Carpenter*'s holding, obtaining a phone or device without a warrant and opening that phone to access its data would constitute an illegal search—that data would be excluded under the Exclusionary Rule. Under the "fruit of the poisonous tree" doctrine, any further evidence gleaned from that data or device or phone (for example, a specific internet search) would be excluded as "fruit" derived from that illegal search.

214. Daniel de Zayas, Comment, Carpenter v. United States *and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 AM. U. L. REV. 2209, 2249 (2019) (quoting *Carpenter*, 138 S. Ct. at 2219).

215. Nardone v. United States, 308 U.S. 338, 341 (1939).

216. *Fruit of the Poisonous Tree*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/fruit_of_the_poisonous_tree (last visited Nov. 20, 2023). "The [fruit of the poisonous tree] doctrine was established in 1920 by the decision in *Silverthorne Lumber Co. v. United States*, and the phrase 'fruit of the poisonous tree' was coined by Justice Frankfurter in his 1939 opinion in *Nardone v. United States*." *Id.* (emphasis added).

217. *Id.*

V. HOW COURTS AND ADVOCATES SHOULD APPROACH THE USE OF PERIOD AND LOCATION DATA

Courts and advocates both should be cognizant of the factual similarities between *Carpenter*'s CSLI and period-tracking and location data used in abortion prosecutions. While the law is still unsettled and only time will tell how *Dobbs* will continue to affect the ways in which data is collected and used in criminal investigations, maintaining the protections guaranteed under the Fourth Amendment as they apply to personal information will be the job of both advocates and the courts. As astutely observed by Cynthia Conti-Cook: "Whether *Carpenter* will protect information related to a pregnant person's web searches for information about their reproductive health [and their period-tracking information] depends on how the courts treat medical information sought online under the third-party doctrine."[218] The third-party doctrine provides an area where the law is not as well established—and where interpretation of the courts will determine the fate of period-tracking data in criminal prosecutions—but the advocacy of individual lawyers will play a crucial role in guiding the courts to decide that fate.

A. The Courts

Courts should approach the use of period-tracking data with hesitation. In a post-*Dobbs* environment where "law enforcement will have access not only to the data available on a subject's phone but also to the extensive personal data available about her from third parties—particularly location data," the state of the law will be determined by whether *Carpenter*'s extension of Fourth Amendment protections to CSLI applies to period-tracking data.[219] Thus far, the scope of *Carpenter*'s application is limited:

> While lower courts are beginning to apply Carpenter's reasoning to facts and circumstances outside of CSLI, it will take time before a full body of law develops and reveals the extent to which *Carpenter* is interpreted to provide Fourth Amendment protections to other kinds of data and the processes

218. Conti-Cook, *supra* note 2, at 44.

219. Jolynn Dellinger & Stephanie Pell, *The Impotence of the Fourth Amendment in a Post-*Roe *World*, LAWFARE (June 13, 2022, 9:06 AM), https://www.lawfareblog.com/impotence-fourth-amendment-post-roe-world.

> that analyze these data. Because *Carpenter*'s reach remains unclear, those involved in any illegal abortion access should assume that law enforcement can obtain access to the data generated through the use of communications technologies and services without a warrant.[220]

Unfortunately, the status of period-tracking app data is left to the mercy of the courts and the advocates representing individuals being prosecuted for illegal abortions. However, the similarities between CSLI and device data cannot be dismissed—and must be emphasized by advocates in these cases.

B. More Advice for Advocates[221]

Advocates should seek to find clarity in *Carpenter*'s logic and "pull from other pre-*Carpenter* cases for principles that promote stronger privacy protections from state surveillance not limited to revealing location data."[222] Advocates should advise their clients—particularly pregnant people—not to voluntarily share their electronic devices with law enforcement.[223] Even if an individual has already shared a device, advocates can find room to argue that "the search conducted lacked knowing and voluntary consent, or was broader than what the person handing over their device believed they consented to."[224] Advocates should feel empowered to draw similarities between period-tracking data and other relevant cases, like *Carpenter*:

> The legal status of pregnant people's reasonable expectation of privacy—while still somewhat undetermined—will challenge advocates to protect their information absent additional state constitutional provisions and state laws protecting the privacy of online information along the same lines as protection for self-incriminating statements under the Fifth Amendment of the U.S. Constitution.[225]

Advocates should seek to find remedy in suppression motions, preventing prosecutions "based on unlawfully obtained

220. *Id.*
221. For previously mentioned advice see *supra* pt. V and pts. IV.A.4. and V.A.
222. Conti-Cook, *supra* note 2, at 44.
223. *Id.* at 47.
224. *Id.*
225. *Id.*

information; private rights of action that will compensate people whose rights have been violated; the ability to sue anonymously to avoid deterring plaintiffs claiming privacy violations; and standing for stakeholder organizations to bring claims on behalf of groups of people whose rights were violated."[226] Data collection from an individual's devices can reveal information so detailed and intimate that it can identify the whereabouts and intentions of those who seek abortions; therefore, advocates must play a crucial role in protecting this personal information.[227]

VI. CONCLUSION

Dobbs overturned fifty years of precedent by concluding that the Constitution does not confer the right to abortion.[228] However, the decision goes beyond the twenty-one states that now ban or mostly ban abortions.[229] While these bans affect those who are pregnant from seeking accessible abortions, disproportionately impacting marginalized communities, an unfortunate and significant consequence of the *Dobbs* decision also relates to data.[230]

Millions of individuals utilize period-tracking apps for myriad purposes: to track their cycles, manage their symptoms, plan for pregnancies, and find awareness around their bodies. [231] This personal information is ripe for mining by law enforcement officials for the purpose of prosecuting individuals for undergoing abortions in states where abortion is now illegal.[232] Given the hodgepodge of federal and state privacy laws[233] in the United States today, the legality of using this data will be left up to the courts to decide and for the advocates who represent individuals in prosecutions of illegal abortions to help dictate.[234]

---

226. *Id.* at 47–48.
227. *Id.* at 48.
228. Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2242 (2022).
229. *See Tracking Abortion Bans Across the Country*, *supra* note 9.
230. *See* Tumulty et al., *supra* note 13.
231. *See* Torchinsky, *supra* note 132.
232. *See id.*
233. *See* Klosowski, *supra* note 156. In the United States, no singular federal law governing data privacy exists; rather, a "mix of laws that go by acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA" govern privacy. *Id.* Unfortunately, as a result: "Most people believe they're protected, until they're not." *Id.* Along with the potpourri of federal laws, there are a handful of state laws—three states have comprehensive consumer privacy laws, including California, Virginia, and Colorado. *Id.*
234. Conti-Cook, *supra* note 2, at 44.

While the Fourth Amendment quite clearly protects individuals from illegal searches and seizures,[235] there is a gray area when it comes to data mined from third parties.[236] Data collected from third parties poses a difficult question for courts as technology and data collection evolve—the information that can now be collected from these entities has become more than mere bank or phone records.[237] Moreover, with the advent and evolution of personal devices, data housed by third parties is becoming ever more prevalent, making the issue of how to categorize data collected from third parties ever more urgent.[238] The urgency to protect this information is compounded by the reality that nearly every individual has one or more personal devices, and those devices house intimate and personal information.[239]

While the Fourth Amendment's protections typically do not extend to information held by third parties, period-tracking and health-related data are sensitive in nature. This data is so ingrained in twenty-first century daily life that it is practically—if not totally—a representation of an individual's thoughts and movements. Because of the reality of our technological moment, where a device may reveal not only an individual's location, but their movements, decisions, and even their thoughts, advocates should feel empowered to argue that *Carpenter* protects this information. The Supreme Court already found that the Fourth Amendment's third-party doctrine does not apply to CSLI, thus, similarly, the Constitution protects the deeply personal nature of what an individual logs into their period app. In other words, through the appropriate advocacy to channel the courts to the right conclusion, the Fourth Amendment's protections extend to period-tracking data by bringing it within the ambit of *Carpenter* and its progeny.

235. U.S. CONST. amend. IV.

236. CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 2 (2022).

237. *See* Torchinsky, *supra* note 132.

238. *See* CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 2 (2022).

239. Conti-Cook, *supra* note 2, at 24, 29.