DATA SURVEILLANCE AND ABORTION BANS AFTER *DOBBS*

Leila Nasrolahi†

TABLE OF CONTENTS

DOI: https://doi.org/10.15779/Z38QV3C51V

† J.D., 2024, University of California, Berkeley, School of Law.

I. INTRODUCTION

Is it acceptable if enforcing criminal law requires us to give up digital privacy? How much of ourselves are we willing to sacrifice for the perfect enforcement of crimes? State laws banning abortions following *Dobbs v. Jackson Women's Health Organization* give rise to these unanswered questions.

In that case, the Supreme Court overturned *Roe v. Wade* and held that the Constitution does not confer a right to abortion.[1] Since then, fourteen states have enacted laws banning almost all abortions, and even more enacted laws placing gestational limits on abortions.[2] In the most hostile states, abortion providers can face up to ninety-nine years in prison—even when the pregnancy was the result of rape or incest.[3]

Much has changed since abortion was last illegal. Most notably, digital technology now pervades reproductive healthcare.[4] Members of the public use the internet to obtain health-related information, period-tracking apps to record their menstrual cycles, GPS to navigate to doctor's appointments, and social media to engage with others on reproductive health topics.[5]

While digital technology provides users with efficient tools for information access, it also provides law enforcement with efficient tools for criminal investigations. In fact, surveillance is the "dominant philosophy for how police enforce laws in 2022."[6] Post-*Dobbs*, there is increasing concern about how pregnant people's digital data will be used against them.[7]

1. Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2284 (2022).

2. *Tracking Abortion Bans Across the Country*, N.Y. TIMES (Nov. 7, 2023), https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html [hereinafter *Tracking Abortion Bans*].

3. *See, e.g.*, ALA. CODE §§ 26-23H-4, 13A-5–6 (2022).

4. *See* Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 UNIV. BALT. L. REV. 1, 24 (2020).

5. *See id.* at 13.

6. Alfred Ng, *'A Uniquely Dangerous Tool': How Google's Data Can Help States Track Abortions*, POLITICO (July 18, 2022), https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906 (explaining how Google's location data can help states track abortions).

7. *See, e.g.*, Jay Edelson, *Post-Dobbs, Your Private Data Will Be Used Against You*, BLOOMBERG L. (Sept. 22, 2022), https://news.bloomberglaw.com/us-law-week/post-dobbs-your-private-data-will-be-used-against-you.

Setting aside the substantive issue of abortion criminalization as an attack on bodily autonomy,[8] this Note describes the "chilling effects"—the over-deterrence of legal activity—that will result from digital data surveillance used in abortion prosecutions. Because there is no viable way to enforce abortion bans via data surveillance without chilling legal activity, this Note argues that abortion bans should not be enforced this way, even if that means settling for lesser enforcement.

This Note proceeds in four Parts. Part II first reviews the Supreme Court's abortion jurisprudence relevant to this piece, namely the trimester framework under *Roe v. Wade*, its modification by the undue burden test in *Planned Parenthood v. Casey*, and finally its subsequent reversal in *Dobbs*. Part II then summarizes the status of state abortion laws to date, paying particular attention to states with the most restrictive bans.

Part III posits that digital data surveillance will be the primary mode of enforcement in abortion actions. In contrast to how abortion laws were enforced pre-*Roe*, Part III describes how data surveillance allows for maximal enforcement. Part IV argues that data surveillance in abortion actions will result in dangerous chilling effects on legal activities. Part V offers solutions and concludes.

II. ABORTION JURISPRUDENCE AND STATE LAWS POST-*DOBBS*

In 1973, the Court held 7-2 that the Due Process Clause of the Fourteenth Amendment protects a fundamental right to privacy, which encompasses the right to an abortion.[9] In *Roe v. Wade*, the Court distinguished between the different stages of pregnancy to delineate how a state could regulate abortion.[10] Before fetal viability, a state could not regulate a person's decision to seek an abortion.[11] Once the fetus reached viability, the point at which it could potentially survive outside the mother's womb, a state could regulate or prohibit abortions except when necessary to save the life of the mother.[12]

8. *See, e.g.*, *The Constitutional Right to Reproductive Autonomy: Realizing the Promise of the 14th Amendment*, CTR. FOR REPRODUCTIVE RTS. (July 2022), https://reproductiverights.org/wp-content/uploads/2022/07/Final-14th-Amendment-Report-7.26.22.pdf (discussing the constitutional rights and guarantees in U.S. law underlying the right to and importance of reproductive autonomy).

9. Roe v. Wade, 410 U.S. 113, 164 (1973).

10. *Id.* at 163–64.

11. *Id.*

12. *Id.*

In 1992, the Court reluctantly reaffirmed *Roe* in *Planned Parenthood of Southeastern Pennsylvania v. Casey*.[13] However, *Casey* discarded the stages-of-pregnancy distinctions from *Roe* and instead imposed the "undue burden" standard, which asked whether a state regulation had the purpose or effect of placing a substantial obstacle in the way of a woman seeking an abortion before viability.[14]

In *Dobbs v. Jackson Women's Health Organization*, the Supreme Court overturned *Roe* and *Casey* and held that the Constitution does not confer a right to abortion.[15] For the first time since 1973, states are empowered to place total, unrestricted bans on abortion.[16] *Dobbs* involved a Mississippi law that generally prohibited abortion after the fifteenth week of pregnancy, well before the viability line announced in *Roe*.[17] In a 6-3 decision, the Court overruled *Roe* and *Casey*, reasoning that the Constitution makes "no reference to abortion, and no such right is implicitly protected by any constitutional provision."[18] Thus, after *Dobbs*, abortion legality is determined by states.

Fourteen states anticipated the reversal of *Roe* and wrote trigger laws banning abortion that immediately took effect after *Dobbs*.[19] In Alabama, Arkansas, Idaho, Indiana, Kentucky, Louisiana, Mississippi, Missouri, North Dakota, Oklahoma, South Dakota, Tennessee, Texas, and West Virginia, abortion is banned with no exceptions for rape or incest.[20] Arizona, Florida, Georgia, Nebraska, North Carolina, and South Carolina, and Utah have gestational limit abortion bans, prohibiting abortion as early as six weeks from the last missed period.[21] Separately, over 100 bills restricting access to abortion were introduced in 2022.[22]

---

13. Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 846, 853 (1992) ("While we appreciate the weight of the arguments made on behalf of the State in the cases before us, arguments which in their ultimate formulation conclude that *Roe* should be overruled, the reservations any of us may have in reaffirming the central holding of *Roe* are outweighed by the explication of individual liberty we have given combined with the force of *stare decisis*.").

14. *Id.* at 879.

15. *Dobbs*, 142 S. Ct. at 2284.

16. *See id.*

17. *Id.* at 2242.

18. *Id.* at 2284.

19. Larissa Jimenez, *60 Days After Dobbs: State Legal Developments on Abortion*, BRENNAN CTR. FOR JUST. (Aug. 24, 2022), https://www.brennancenter.org/our-work/research-reports/60-days-after-dobbs-state-legal-developments-abortion.

20. *Tracking Abortion Bans*, *supra* note 2.

21. Amy Schoenfeld Walker, *Most Abortion Bans Include Exceptions. In Practice, Few Are Granted*, N.Y. TIMES (Jan. 21, 2023), https://www.nytimes.com/interactive/2023/01/21/us/abortion-ban-exceptions.html.

22. Jimenez, *supra* note 19.

On the other side, several progressive states introduced legislation to expand abortion coverage following the *Dobbs* decision. In 2023, at least sixteen states passed legislation protecting abortion access.[23] New Jersey passed a bill to codify a constitutional right to freedom of reproductive choice.[24]

III. DATA SURVEILLANCE WILL BE THE PRIMARY MODE OF ENFORCING ABORTION BANS

Data surveillance will be the primary mode of enforcement of abortion bans because: (1) it captures the widest possible range of potential criminal activity; (2) it answers questions that even medicine cannot; and (3) there is already evidence of it being used.

Dobbs must be considered against the backdrop of unprecedented technological advances in data surveillance[25] that have developed since *Roe*—technologies that allow law enforcement to achieve the most capacious mode of enforcement. That is, modern data surveillance captures as much potential criminal activity as possible—what I refer to as "maximal enforcement." Data surveillance offers law enforcement an efficient and effective way to track criminal activity.[26] This is especially relevant in the abortion context since the activity at issue is inherently intimate and private. Moreover, digital data can answer a question about abortions that even medicine cannot: the difference between a medical abortion and a miscarriage.[27] That is, since the abortion pill

23. *Id.*

24. N.J. STAT. ANN. § 10:7-1(a).

25. Since *Roe*, Google was founded in 1998, portable GPS devices became available in 1999, Facebook was founded in 2004, and the first iPhone was sold in 2007. With that, increasing connections between technology and policing have developed. *See From the Garage to the Googleplex*, ABOUT GOOGLE, https://about.google/intl/ALL_us/our-story/ (last visited Nov. 11, 2023); Geotab Team, *History of GPS Satellites and Commercial GPS Tracking*, GEOTAB (June 23, 2020), https://www.geotab.com/blog/gps-satellites/; Nicholas Carlson, *At Last—The Full Story of How Facebook was Founded*, BUS. INSIDER (Mar. 5, 2010), https://www.businessinsider.com/how-facebook-was-founded-2010-3); Ben Gilbert & Sarah Jackson, *Steve Jobs Unveiled the First iPhone 16 Years Ago—Look How Primitive It Seems Today*, BUS. INSIDER (Jan. 9, 2023), https://www.businessinsider.com/first-phone-anniversary-2016-12). For research suggesting that technological improvements have increased police capabilities, see CHRISTOPHER KOPER, CYNTHIA LUM, JAMES WILLIS, DAN WOODS & JULIE HIBDON, REALIZING THE POTENTIAL OF TECHNOLOGY IN POLICING: A MULTISIDE STUDY OF THE SOCIAL, ORGANIZATIONAL, AND BEHAVIORAL ASPECTS OF IMPLEMENTING POLICING TECHNOLOGIES (2015), https://nij.ojp.gov/library/publications/realizing-potential-technology-policing-multisite-study-social-organizational.

26. *See infra* Section III.B.

27. The abortion pill works by stimulating the same process as a naturally occurring miscarriage. *See* Jessica Beaman, Christine Prifti, Eleanor Bimla Schwarz & Mindy Sobota,

stimulates the same process as a naturally occurring miscarriage, a doctor cannot readily discern whether a patient who is purporting to have a miscarriage in fact took an abortion pill. However, that patient's search history and location data may provide an answer.

Today's surveillance technology is what will separate pre-*Roe* abortion bans from post-*Dobbs* bans. Whereas abortion bans pre-*Roe* depended on physical evidence to prosecute lawbreakers, today digital data surveillance will be the primary mode of enforcing abortion bans.[28]

A. PRE-*ROE* ENFORCEMENT

Dobbs must be considered in light of the unprecedented technological advances in data surveillance that have taken place since *Roe*. It is helpful to first understand enforcement mechanisms pre-*Roe* as a contrast to the pervasive possibilities that data surveillance now offers.

In the early 1900s, before data surveillance was available as an enforcement mechanism, abortion laws were enforced primarily through obtaining dying declarations of women who received abortions and through police raids.[29] When a woman in the early twentieth century died from an illegal abortion, the state prosecuted the "abortionist" by using dying declarations as a crucial piece of evidence.[30] In fact, some thought that without the dying declaration, it was "almost 'impossible' to obtain evidence of criminal abortion any other way."[31] Since early abortions practices were often unsafe and performed illegally by non-physicians, women often called their physicians when they experienced post-abortion complications.[32] Prosecutors primarily focused on cases where women died and were considered "victims" of a crime.[33] When this happened to Carolina Petrovitis, her doctor asked, "Who did it for you[?] If you won[']t tell me what was done to you I can't handle your case."[34] Petrovitis eventually revealed that a midwife performed her abortion and her doctor informed police officers.[35] As Petrovitis realized she would soon die,

Medication to Manage Abortion and Miscarriage, 35 J. GEN. INTERNAL MED. 2398 (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7403257/ (noting that "for both medication abortion and medical management of early miscarriage, the standard of care is to provide oral mifepristone followed by misoprostol tablets").

28. *Infra* Section III.B.

29. LESLIE J. REAGAN, WHEN ABORTION WAS A CRIME: WOMEN, MEDICINE, AND LAW IN THE UNITED STATES, 1867–1973, at 114, 161 (1997).

30. *Id.* at 114.

31. *Id.* at 118.

32. *See id.* at 119.

33. *Id.* at 116.

34. *Id.* at 113.

35. *Id.*

the police collected a statement that implicated the midwife who performed her abortion.[36] The police brought the midwife to the hospital and Petrovitis identified her as the person who performed her illegal abortion.[37]

To gather evidence to prosecute abortionists in the early 1900s, the state needed to have physicians reporting abortions and collecting dying declarations from their patients, which many doctors were reluctant to do.[38] But doctors were convinced to side with the state because they feared the investigative process would be "turned against them."[39] This fear was not irrational; records from medical society meetings describe doctors' experiences being indicted as an accessory to murder for failing to call the coroner or obtain a dying declaration from a patient.[40] Even when doctors were acquitted of abortion charges, they were excommunicated by their medical communities.[41] To protect themselves, physicians were advised to "deny medical care to a woman who had had an abortion until she made a statement."[42] As a result, "doctors found themselves caught in the middle between their responsibilities to their patients and the demands of government officials."[43]

In addition to dying declarations, by the 1940s the state relied on aggressive raids to enforce abortion laws. Rather than only focusing on women's deaths by unsafe abortionists, prosecutors "worked to shut down the trusted and skilled abortionists, many of them physicians, who had operated clinics for years with little or no police interference."[44] Consider the story of an underground abortion clinic in Pennsylvania. After receiving a tip from a suspicious neighbor,

> police officers . . . hid in the nearby fields . . . waiting and watching . . . . [T]he officers unlocked the front door . . . . [T]hey found one woman wearing only a slip in one room, two lying in bed in another, and two more who, having removed their skirts and underwear, sat waiting for their abortions in a third.[45]

36. *Id.*
37. *Id.*
38. *Id.* at 120.
39. *Id.*
40. *Id.* at 120–21.
41. *Id.*
42. *Id.* at 122.
43. *Id.* at 116.
44. *Id.* at 161.
45. Leslie J. Reagan, *Caught in the Net*, SLATE (Sept. 10, 2021), https://slate.com/news-and-politics/2021/09/enforcement-of-abortion-laws-before-roe-v-wade.html.

These raids were the primary mode of enforcement in the 1950s and 1960s.[46] Police officers raided offices and apartments where abortion providers worked and escorted women to male doctors who would determine whether a surgical procedure had been performed.[47] Doctors would then testify in court as to their findings.[48] Meanwhile, the women who received abortions were forced to testify in court against their abortion provider.[49]

Pre-*Roe* enforcement tools relied on physical confrontations that took place after abortion care was administered. Much has changed since then. Whereas in the early 1900s it may have been impossible to imagine abortion prosecutions without dying declarations,[50] today's digital age allows law enforcement to obtain a wealth of information without relying on physical confrontation and well before an abortion occurs.

B. POST-*ROE* ENFORCEMENT

Data surveillance is a promising way to determine whether someone had or is planning to have an abortion because of how pervasive and informative the data is. Search history data provides information about a person's thoughts and considerations before any actions have necessarily been taken. Location data provides information connected to one's movements—where they go and when they go.[51] Data from reproductive health applications, websites, and social media pages provides information specific to abortion care.[52] This data about a person is produced "as an unintended byproduct of access to internet search tools, social-media platforms and other communication apps, and web-based services to make purchases or access services via a smartphone or other wired device."[53] Data surveillance gives information about "individuals' physical states, movements, interests, and moods on a minute-by-minute basis."[54]

This Section, III.B, discusses three categories of data surveillance that are relevant to abortion criminal law enforcement. First, the data from search history that reveals the user's thoughts; second, location data that follows users' physical movements; and lastly, medical data that offers concrete

46. REAGAN, *supra* note 29, at 160–62.
47. *Id.*
48. *Id.*
49. *Id.* at 165.
50. *Id.* at 118.
51. *Infra* notes 66–76.
52. *Infra* notes 77–86.
53. Aziz Z. Huq & Rebecca Wexler, *Digital Privacy for Reproductive Choice in the Post-Roe Era*, 98 N.Y.U. L. REV. 555, 569–70 (2023).
54. *Id.* at 570.

information about pregnancy, menstruation, and other markers of reproductive health.

1. Modern Digital Data Technologies Reveal the User's Thoughts Before They Act on Them.

Search history data allows an evidence trail to begin much earlier than ever before—Google might be the first to find out someone is pregnant. Our search history is an extension of our thoughts.[55] *What do my symptoms mean? How much does an abortion cost?* Our online data follows our most intimate wonderings, blurring the lines between our physical and digital selves.[56] Pregnant people are likely to search for health-related information online, especially during the early stages of pregnancy.[57] Pregnant people "prefer the online experience because of . . . the ability to manage their health in what feels like a private manner."[58] Search history sheds light on the questions people may be too afraid to ask in-person.

Law enforcement can require Google to turn over search history data by using a "keyword warrant." A keyword warrant is when police request data in "reverse" by asking Google to disclose everyone who searched a keyword, without necessarily having a specific suspect in mind.[59] For example, in a 2020 arson-murder investigation, police sent a search warrant requesting information on users who searched the address of the residence around the time of the arson.[60] Google complied with the data request, and three teenagers who searched the address were charged with murder.[61] In a fraud investigation, police requested "any/all user or subscriber information related to the Google searches of 'Douglas [REDACTED]' for the timeframe of December 1st, 2016 thru January 7th, 2017."[62] The warrant specified that the

55. SETH STEPHENS-DAVIDOWITZ, EVERYBODY LIES: BIG DATA, NEW DATA, AND WHAT THE INTERNET CAN TELL US ABOUT WHO WE REALLY ARE (2017).

56. *Id.*

57. *See generally* Padaphet Sayakhot & Mary Carolan-Olah, *Internet Use by Pregnant Women Seeking Pregnancy-Related Information: A Systematic Review*, BMC PREGNANCY CHILDBIRTH (Mar. 28, 2016), https://pubmed.ncbi.nlm.nih.gov/27021727/.

58. Conti-Cook, *supra* note 4, at 24.

59. Alfred Ng, *Google Is Giving Data to Police Based on Search Keywords, Court Docs Show*, CNET (Oct. 8, 2020), https://www.cnet.com/news/privacy/google-is-giving-data-to-police-based-on-search-keywords-court-docs-show/.

60. Julia Love, *Google Keyword-Search Warrants Questioned by Colorado Lawyers*, BLOOMBERG (Jan. 12, 2023), https://www.bloomberg.com/news/articles/2023-01-12/google-keyword-search-warrants-questioned-by-colorado-lawyers.

61. *Id.*

62. Application for Search Warrant, No. 27-CR-CV-17-1 (Feb. 1, 2017), https://www.documentcloud.org/documents/3519211-Edina-Police-Google-Search-Warrant-Redacted.html.

information should include names, addresses, phone numbers, dates of birth, social security numbers, email addresses, payment information, account information, and IP addresses of all persons who made the Google search.[63] In each of these scenarios, law enforcement used keyword warrants to obtain critical search history data.

Search history evidence is not new, but post-*Dobbs* abortion bans give it new power. When Latice Fisher was prosecuted for second-degree murder for the death of her newborn after stillbirth, her online search, "buy Misopristol Abortion Pill Online," was key evidence.[64] In future abortion investigations, law enforcement can utilize a reverse keyword search to locate individuals who searched "Planned Parenthood address" or "abortion pills"—without having any specific suspect in mind. Albert Fox Cahn, the executive director of the Surveillance Technology Oversight Project, likened keyword warrants to "going to a library and then trying to search every person who checked out a specific book," arguably something we "would never allow . . . in the analog world."[65]

2. Moving Data Trails

In addition to our intimate thoughts, our digital data also follows our physical movements. Many cellphone applications enable "location services," which provide information about the geographic position of the device, even when the app is not actively being used.[66] Google tracks location data from the IP address of a device's internet connection, a web search that includes a location in it, and Google Maps usage. Location-based data and analytics can identify where users are traveling from, how often they are visiting a location, and traveler demographics.[67] Location History logs a user's location on average every two minutes.[68] By using geofencing technology, companies can direct advertisements at smartphone users located in a designated area through browsers and applications on their devices.

63. *Id.*

64. *See* Conti-Cook, *supra* note 4, at 3 n.3.

65. Bobby Allyn, *Privacy Advocates Fear Google Will be Used to Prosecute Abortion Seekers*, NPR (July 11, 2022), https://www.npr.org/2022/07/11/1110391316/google-data-abortion-prosecutions.

66. *Location, Location, Location: Tips on Controlling Mobile Tracking*, ST. CAL. DEP'T JUST.: OFF. ATT'Y GEN. (Oct. 2015), https://oag.ca.gov/privacy/facts/online-privacy/location.

67. Emily Carroll, *What is Location-Based Data?*, DRIVERESEARCH (July 8, 2019), https://www.driveresearch.com/market-research-company-blog/what-is-location-based-data-market-research-company/.

68. Cullen Seltzer, *Google Knows Where You've Been. Should It Tell the Police?*, SLATE (May 16, 2022), https://slate.com/technology/2022/05/google-geofence-warrants-chatrie-location-tracking.html.

Even before *Dobbs*, digital data was used to monitor and target individuals who sought abortions. For example, in 2017, Copley Advertising created mobile geofences at reproductive health centers that read "Pregnancy Help," "You Have Choices," and "You're Not Alone."[69] Copley was hired by pro-life religious groups to target "abortion-minded" women.[70]

By obtaining geofence warrants, police can make requests to Google for data on devices logged in at a specific area and time.[71] Google received 982 geofence warrants in 2018, 8,396 in 2019, and 11,554 in 2020.[72] Google does not publish information about how often it complies with geofence warrants or whether it rejects overly broad requests.[73] Geofence warrants, like keyword warrants, are "reverse" warrants because they identify people—anyone—who was near a certain area in a specified time frame. A geofence warrant "doesn't start with a suspect or even an account; instead police request data on every device in a given geographic area during a designated time period, regardless of whether the device owner has any link at all to the crime under investigation."[74] Police have used geofence warrants to determine the suspects in a burglary[75] and attendees at a protest.[76] Rather than conducting a physical raid to prove someone received an abortion, today police can draw a 200-foot boundary around an abortion clinic and use Google location data to determine the identity of everyone who entered the area at any given moment.

3. Data Trails Specific to Reproductive Health

In addition to the general information offered by search history and location tracking, there is an amalgam of digital data specific to reproductive

69. *AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities*, MASS.GOV (Apr. 4, 2017), https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities.

70. *Id.*

71. *Id.*

72. Zack Whittaker, *Google Says Geofence Warrants Make Up One-quarter of All US Demands*, TECHCRUNCH (Aug. 19, 2021), https://techcrunch.com/2021/08/19/google-geofence-warrants/.

73. *Id.*

74. Jennifer Lynch, *First Court in California Suppresses Evidence from Overbroad Geofence Warrant*, ELEC. FRONTIER FOUND. (Oct. 11, 2022), https://www.eff.org/deeplinks/2022/10/california-court-suppresses-evidence-overbroad-geofence-warrant.

75. Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2508 (2021).

76. Matthew Guariglia, Mukund Rathi, Houston Davidson & Jennifer Lynch, *Geofence Warrants Threaten Civil Liberties and Free Speech Rights in Kenosha and Nationwide*, ELEC. FRONTIER FOUND. (Sept. 10, 2021), https://www.eff.org/deeplinks/2021/09/geofence-warrants-threaten-civil-liberties-and-free-speech-rights-kenosha-and.

health. As of the last decade, there has been an explosion of *femtech*[77] tools, products, services, wearable technology, and software that "use technology to address women's health issues, including menstrual health, reproductive health, sexual health, maternal health and menopause."[78] Femtech apps like Flo (a menstrual tracking app), Glow (a fertility tracking app), and Ava (a fertility tracking bracelet) store data about users that is specific to their reproductive health, including menstruation data and sexual activity. Period tracking apps are a common tool for people to anticipate their cycle symptoms, log menstruation dates, and family-plan. Some apps can predict pregnancy more than a week before at-home pregnancy tests can.[79] One study found that nearly a third of women in the United States use a period-tracking app.[80] Flo, a popular app with millions of users, includes articles, quizzes, and even a community for discussing sexual and reproductive health issues.[81] Post-*Dobbs*, experts say period-tracking data may become a target for investigators.[82] Used in combination with search history and location data, a period tracking app may give law enforcement evidence that someone received an illegal abortion.

Another critical change since the *Roe* era is the way digital communications are captured on social media. Social media is increasingly used as a source of political news and discussion.[83] Countless Instagram accounts specifically offer abortion-related content, offering anything from mutual aid funds, political opinions, personal stories, and information to obtain abortions in states where it is illegal.[84] Law enforcement is already using social media data in abortion

77. "Femtech" was coined by Ida Tin, co-founder of Clue, a menstrual health app. Ida Tin, *The Rise of a New Category: Femtech*, CLUE (Sept. 14, 2016), https://helloclue.com/articles/culture/rise-new-category-femtech.

78. Linda Rosencrance, *What Is Femtech?*, TECHTARGET (Apr. 2022), https://www.techtarget.com/whatis/definition/femtech.

79. Huq & Wexler, *supra* note 53, at 573.

80. Carly Page, *Supreme Court Overturns Roe v. Wade: Should You Delete Your Period-Tracking App?*, TECHCRUNCH (May 5, 2022), https://techcrunch.com/2022/05/05/roe-wade-privacy-period-tracking/.

81. *See* FLO HEALTH, https://flo.health/ (last visited Nov. 22, 2023).

82. *See, e.g.*, Leah Fowler & Michael Ulrich, *Femtechnodystopia*, 75 STAN. L. REV. 1233, 1313 (2023) ("Period- and fertility-tracking apps are the most obvious consumer technologies but by no means the only ones that could be instrumentalized to criminalize abortion and other behaviors during pregnancy.").

83. Dam Hee Kim, Brian E. Weeks, Daniel S. Lane, Lauren B. Hahn & Nojin Kwak, *Sharing and Commenting Facilitate Political Learning on Facebook: Evidence From a Two-Wave Panel Study*, 7 SOC. MEDIA + SOC'Y (Sept. 27, 2021), https://journals.sagepub.com/doi/full/10.1177/20563051211047876.

84. *See, e.g.*, Nat'l Network of Abortion Funds (@abortionfunds), INSTAGRAM, https://www.instagram.com/abortionfunds/ (last visited Nov. 22, 2023); Liberate Abortions (@liberateabortion), INSTAGRAM, https://www.instagram.com/liberateabortion/ (last visited

investigations. For example, a Nebraska mother was sentenced to two years in prison for giving abortion pills to her pregnant daughter after 20 weeks of pregnancy.[85] Law enforcement obtained a warrant for their Facebook messages which allegedly discussed their plans to terminate the pregnancy at home.[86]

In just the first half of 2021, Google received approximately 150,000 government requests for disclosure of users' account information pursuant to a subpoena in all cases and a search warrant in criminal cases.[87] Google complied with almost 80% of those requests.[88] Apple received 12,589 government requests and complied in 90% of cases.[89] Facebook received 237,414 requests and provided data in 76.1% of cases.[90] Data-driven law enforcement "lets police become aggressively more proactive."[91] A supervising police detective said, "tech providers, especially social media platforms, offer a trove of information that can help solve [crimes]. Everything happens on Facebook. The amount of information you can get from people's conversations online—it's insane."[92]

Combined, all the data that companies collect from their users make up what has been coined as "surveillance capitalism": "the unilateral claiming of private human experience as free raw material for translation into behavioral data."[93] So long as these surveillance mechanisms exist, law enforcement and

---

Nov. 22, 2023); Abortion Photograph (@theabortionproject), INSTAGRAM, https://www.instagram.com/theabortionproject/ (last visited Nov. 22, 2023).

85. Margery A. Beck, *Nebraska Mother Sentenced to 2 years in Prison for Giving Abortion Pills to Pregnant Daughter* AP NEWS (Sept. 22, 2023, 2:31 PM), https://apnews.com/article/abortion-charges-nebraska-sentence-36b3dcaadd6b705ca2315bc95b99bdc1.

86. *Id.*

87. *Global Requests for User Information*, GOOGLE: TRANSPARENCY REP., https://transparencyreport.google.com/user-data/overview (last visited Nov. 22, 2023).

88. *Id.*

89. APPLE, APPLE TRANSPARENCY REPORT: GOVERNMENT AND PRIVATE PARTY REQUESTS 1 (2021), https://www.apple.com/legal/transparency/pdf/requests-2021-H1-en.pdf ("Types of legal requests Apple receives from the United States can be: subpoenas, court orders, search warrants, pen register/trap and trace orders, or wiretap orders.").

90. *Facebook Transparency Report*, FACEBOOK, https://transparency.fb.com/data/government-data-requests/ (last visited Nov. 22, 2023).

91. *How Data-driven Policing Threatens Human Freedom*, ECONOMIST (June 4, 2018), https://www.economist.com/open-future/2018/06/04/how-data-driven-policing-threatens-human-freedom.

92. Matt O'Brien & Michael Liedtke, *How Big Tech Created a Data 'Treasure Trove' for Police*, COURTHOUSE NEWS SERV. (June 22, 2021), https://www.courthousenews.com/how-big-tech-created-a-data-treasure-trove-for-police/.

93. Shoshana Zuboff, a professor at Harvard Business School, coined the term "surveillance capitalism" in 2014. Zuboff notes it was "Google that first learned how to capture surplus behavioral data, more than what they needed for services, and used it to

private enforcers will continue to take full advantage of available data**.** As the saying goes, "if you build it, they will come."

4. Data is Easy for Law Enforcement to Obtain

It will not be difficult for law enforcement to access the troves of data created by our digital devices. To obtain a warrant for users' data, police must satisfy a probable cause showing. However, "warrants will offer only very limited protection against restrictionist law enforcement demands" because probable cause is such a low bar.[94] Police who seek a keyword warrant for users who searched "abortion" will likely be able to articulate probable cause just by "point[ing] to criminal statutes in seeking evidence about abortion."[95]

Police can also circumvent warrant requirements by purchasing data directly from data brokers. Widespread data surveillance supports what is known as a data economy, a "digital ecosystem in which the producers and consumers of data—business and individuals—and government and municipal agencies gather, organize, and share accumulated data from a wide variety of sources."[96] Users' data is pervasively shared and sold to third party data brokers who compile it and resell it to whoever seeks to buy it—including individuals, advertisers, marketing firms, and law enforcement.[97] In August 2022, the Federal Trade Commission sued Kochava Inc., a data broker allegedly selling non-anonymized mobile geolocation data that could be used to track consumers' visits to sensitive locations including abortion providers.[98] To prove how easy it is to obtain location data of people who visit abortion clinics, a reporter bought a week's worth of data on where people who visited

compute prediction products that they could sell to their business customers, in this case advertisers." John Laidler, *High Tech is Watching You*, HARV. GAZETTE (Mar. 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/.

94. Huq & Wexler, *supra* note 53, at 578.

95. *Id.*

96. *Capitalizing on the Data Economy*, MIT TECH. REV. (Nov. 16, 2021), https://www.technologyreview.com/2021/11/16/1040036/capitalizing-on-the-data-economy/.

97. *See, e.g.*, Bennett Cyphers, *Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police.

98. *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations*, FED. TRADE COMMISSION (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

Planned Parenthood came from and went afterward for just $160 from a data broker called SafeGraph.[99]

Law enforcement—and anyone else—can purchase data directly from data brokers without any judicial oversight. One data broker, Fog Data Science, contracts with police to provide "easy and often warrantless access to the precise and continuous geolocation of hundreds of millions of unsuspecting Americans."[100] Fog purchases billions of data points across thousands of mobile apps from millions of devices, which it then sells to law enforcement agencies for a cheap subscription fee.[101]

Post-*Dobbs* abortion law enforcement will look drastically different from the rudimentary pre-*Roe* methods. An overwhelming amount of information about individuals' thoughts, ideas, preferences, and movements is collected by Big Tech companies. Law enforcement will capitalize on this data to identify as much abortion-related activity as possible.

C. DIGITAL DATA ANSWERS QUESTIONS THAT EVEN MEDICINE CANNOT

Data surveillance is a feasible way to determine whether someone is planning to have an abortion. Unless a pregnant person specifically goes out of their way to avoid a digital trace completely, their location data and search history will implicate them. Data surveillance offers law enforcement the tools to achieve as close to perfect enforcement as possible. Moreover, digital data answers a question that medicine often cannot: the difference between a miscarriage and a medical abortion. From a medical perspective, "there is no physically significant difference between a medication abortion and a spontaneously occurring miscarriage. For example, the medicines used in medication abortion are used to help safely manage an incomplete miscarriage."[102] Digital data has the power to fill in the gaps. In states where abortion is banned, consider the following scenario: a pregnant person takes an abortion pill and experiences excessive bleeding. She goes to her doctor but does not want to disclose that she took abortion pills. Her doctor provides

99. Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

100. Matthew Guariglia, *What Is Fog Data Science? Why Is the Surveillance Company So Dangerous?*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/06/what-fog-data-science-why-surveillance-company-so-dangerous.

101. *Id.*

102. *Consumer Health Info: Medication Abortion and Miscarriage*, NAT'L WOMEN'S HEALTH NETWORK (Aug. 15, 2019), https://nwhn.org/abortion-pills-vs-miscarriage-demystifying-experience/.

treatment—the same treatment used for both abortions and miscarriage. Perhaps the doctor is suspicious that it was a self-managed abortion but cannot diagnose because there is no way to distinguish from a spontaneous miscarriage. But her search history shows searches for abortion pills. Geolocation data places her at a clinic that was known to provide abortions before *Dobbs*. Suddenly, her digital data enables a medical diagnosis.

IV. CHILLING EFFECTS

Part III described the pervasive data surveillance that will be used in abortion-related criminal investigations. This Part considers the repercussions of that surveillance, which I argue are chilling effects on various legal activities. I use "chilling effects" to mean that a rule will involve some ambiguity or error in application, causing people to avoid beneficial conduct that society would otherwise like them to engage in.

The "chilling effect" is a phenomenon in which people refrain from engaging in legal expression for fear of breaking a law and the subsequent retaliation, prosecution, or punitive governmental action.[103] In states where abortion bans are in place, people will be deterred from breaking criminal abortion laws, but they will also refrain from participating in legal activities like providing life-saving abortions and sharing information about reproductive health.[104] Law enforcement's use of data surveillance—the enforcement mechanism—will be the primary cause of this deterrence, rather than the severity of punishment itself. Criminal deterrence scholars have posited that the *certainty of punishment* has a greater impact on deterrence than the *severity of punishment*:

> Certainty refers to the likelihood of being caught and punished for the commission of a crime. Research underscores the more significant role that certainty plays in deterrence than severity—certainty of being caught deters a person from committing crime, not the fear of being punished or the severity of the punishment. Effective policing that leads to swift and certain (but not necessarily severe) sanctions is a better deterrent than the threat of incarceration.[105]

103. David L. Hudson, Jr., *Chilling Effect Overview*, FOUND. FOR INDIVIDUAL RTS. & EXPRESSION, https://www.thefire.org/research-learn/chilling-effect-overview.

104. *See, e.g.*, *Further Restricting Abortions in NC Will Have 'Chilling' Effect, Doctors Say*, DUKE TODAY (Feb. 17, 2023), https://today.duke.edu/2023/02/further-restricting-abortions-nc-will-have-chilling-effect-doctors-say.

105. *Five Things About Deterrence*, NAT'L INST. JUST. (June 5, 2016), https://nij.ojp.gov/topics/articles/five-things-about-deterrence.

Applying this logic, the probability of whether someone will be caught performing or receiving an abortion has a greater impact on behavior than the length of the sentence imposed. Since the probability of punishment is determined by the pervasiveness of data surveillance, it follows that the more surveillance there is, the more behavior—both legal and illegal—will be deterred. The likelihood of enforcement in the abortion context is dependent on the invasiveness of digital surveillance.[106] Without it, enforcement mechanisms will look like they did pre-*Roe* and will be inefficient and largely ineffective. Therefore, without a fine net of data, the concerns of the chilling effects described below would be much less. Conversely, the more data surveilled, the greater the chilling effects will become.

Data surveillance as an enforcement mechanism for abortion bans gives rise to three major chilling effects. First, there will be a chilling effect on legal abortion access. Second, there will be a chilling effect on legal non-abortion reproductive care. Third, there will be a chilling effect on legal information sharing about reproductive health. Each is discussed in turn.

A. DATA SURVEILLANCE WILL CHILL ACCESS TO LEGAL ABORTION CARE

Data surveillance will have a chilling effect on legal abortions because increasing the certainty of enforcement will make doctors more risk averse to perform abortions in gray areas. As they stand, abortion laws target providers and others who assist in performing an abortion.[107] But even the strictest states have exceptions when abortion is necessary to save the life of the mother.[108] Other less restrictive states also include exceptions when the pregnancy was the result of rape or incest.[109] As abortion laws are more intensely enforced via data surveillance, these important exceptions will be undermined because doctors will be fearful of being wrongfully accused of performing an illegal abortion.[110]

In 2021, Alabama made it a Class A felony to perform an abortion except in cases where it is necessary to "prevent a serious health risk to the unborn child's mother," which the legislature defined as death or serious risk of substantial physical impairment of a major bodily function.[111] Class A felonies are punishable by up to ninety-nine years in prison.[112] Therefore, there will be

106. *See supra* Part III.
107. *See, e.g.*, ALA. CODE § 26-23H-4 (2021); IDAHO CODE § 18-622 (2020).
108. *See* statutes cited *supra* note 107.
109. *See* Walker, *supra* note 21.
110. *See id.*
111. ALA. CODE §§ 26-23H-4–8 (1975).
112. ALA. CODE §§ 13A-5–6 (2019).

instances in which doctors must ask and answer questions like: *Is this patient's condition close enough to death? How much blood loss must occur before an ectopic pregnancy is considered life-threatening under Alabama's law? How serious is a "serious risk"? How should "substantial" impairment be quantified?*[113] These are all questions that remain unanswered and will inevitably unfold as cases are litigated. What if, in investigating whether the mother's life was truly endangered, law enforcement obtains search history data that indicates the woman was seeking an abortion?

Several doctors have articulated their fears. One Indiana doctor described a patient whose ultrasound showed a miscarriage was inevitable and the mother's life was potentially in danger, but Kentucky doctors refused to terminate the pregnancy.[114] In Kentucky, abortion is completely banned except for when necessary to save the mother's life.[115] The patient was able to travel to Indiana, where doctors were able to "provide that pregnancy termination for her, save her uterus, and potentially save her life."[116] Even though the patient's pregnancy could not continue, and her life was potentially in danger, Kentucky doctors "did not feel that they were legally able to [terminate the pregnancy]. So they sent her away."[117]

In Ohio, Tara George's ultrasound showed there was no amniotic fluid around the fetus, indicating that the fetus was in kidney failure and had multiple heart defects.[118] Before Ohio's recent amendment to its constitution,[119] it banned abortions after six weeks, except to prevent the death of the mother or the serious risk of substantial and irreversible impairment of a major bodily function.[120] If Tara carried the fetus to term, it would survive for no more than a few hours. Doing so would also put Tara's life at risk, since she had various medical conditions that put her "at high risk for hemorrhaging, clotting and preeclampsia—all potentially deadly complications."[121] Tara's best

113. J. David Goodman & Azeen Ghorayashi, *Women Face Risks as Doctors Struggle With Medical Exceptions on Abortion*, N.Y. TIMES (July 20, 2022), https://www.nytimes.com/2022/07/20/us/abortion-save-mothers-life.html.

114. *Doctors Refusing Potentially Life-saving Abortion Treatment Over Legal Fears, Indiana Doctor Says*, ABC NEWS (Aug. 24, 2022), https://www.radioalabama.net/news/national/doctors-refusing-potentially-life-saving-abortion-treatment-over-legal-fears-indiana-doctor-says.

115. KY. REV. STAT. ANN. § 311.723 (West 2019).

116. *Doctors Refusing Potentially Life-saving Abortion Treatment Over Legal Fears*, *supra* note 114.

117. *Id.*

118. Elizabeth Cohen & Danielle Herman, *Ohio's New Abortion Law Forces Doctor to Fight to Protect Her Patient's Life*, CNN (Sept. 22, 2022), https://www.cnn.com/2022/09/22/health/ohio-abortion-patient-doctor/index.html.

119. Julie Carr Smyth, *Ohio Voters Just Passed Abortion Protections, When and How They Take Effect is Before the Courts*, AP NEWS (Nov. 24, 2023), https://apnews.com/article/abortion-ohio-constitutional-amendment-republicans-courts-fb1762537585350caeee589d68fe5a0d.

120. S.B. 23, 133rd Gen. Assem. (Ohio 2019).

121. Cohen & Herman, *supra* note 118.

option was to terminate the pregnancy, but Ohio hospital lawyers advised her doctor not to do so because there was uncertainty as to "how sick is sick enough."[122] Since doctors could lose their medical license, face fines, and be incarcerated for performing an illegal abortion, "doctors and hospitals are reluctant to get even close to violating it."[123] Life-saving abortions are legal and desirable, but the risk of it being miscategorized as an illegal abortion deters doctors who are reasonably fearful of the criminal liability.

In addition to life-saving exceptions, some state laws allow abortions in cases of rape or incest. Although these abortions are legal, doctors must decide whether their patients' claims are valid. Abortion clinics across these states have noted, "while the law may allow people to terminate their pregnancy in those instances, it will likely be easier to get patients across state lines for an abortion than try to clear the hurdles associated with obtaining one legally in their home state."[124] One provider in Wyoming's only clinic said, "I don't want to go to jail. I don't want to break the law, but I also can't imagine a patient who has been raped or assaulted and is pregnant and calling for help and, as a gynecologist, to say to her, 'Sorry, you're on your own.' It's just horrific."[125] The same experience has occurred in Texas, where some physicians with training in abortion procedures have been unable to offer even abortions allowed by SB8 because nurses and anesthesiologists, concerned about being seen as "aiding and abetting," have declined to participate.[126]

The better data surveillance is at capturing abortion, the more likely it is that doctors will be chilled from engaging in legal, desirable behavior. A pregnant person's digital search for abortion-inducing medication, location data revealing presence at a reproductive health clinic, and information from a period tracking app can all be deployed in criminal proceedings. Since doctors are the primary target of these criminal laws, knowing that law enforcement has the capacity to track their patients' locations, desires, and plans via their digital data will cause doctors to feel hyperaware that their decision-making process can be readily scrutinized.

122. *Id.*

123. *Id.*

124. Megan Messerly, *In States That Allow Abortion for Rape and Incest, Finding a Doctor May Prove Impossible*, POLITICO (June 27, 2022), https://www.politico.com/news/2022/06/27/abortion-exceptions-doctor-shortage-00042373.

125. *Id.*

126. Whitney Arey, Klaira Lerma, Anitra Beasley, Lorie Harper, Ghazaleh Moayedi & Kari White, *A Preview of the Dangerous Future of Abortion Bans—Texas Senate Bill 8*, 387 NEW ENG. J. MED. 388, 388–89 (2022).

B. DATA SURVEILLANCE WILL CHILL THE PROVISION OF LEGAL HEALTH CARE

Second, data surveillance for abortion ban enforcement will have a chilling effect on the provision of legal health care because many medications that treat a variety of non-abortion-related conditions have side-effects related to pregnancy. Rheumatoid arthritis patients use methotrexate, which can cause miscarriage or serious birth defects, for pain relief.[127] Mifepristone—the pill given for medication abortions—is also used to manage miscarriages, treat cancer, and control hyperglycemia in patients with Type 2 diabetes.[128] Isotretinoin treats severe acne, but causes severe birth defects.[129] Of course, treating arthritis, miscarriages, cancer, and skin conditions is completely legal and desirable activity. Nevertheless, increasing the certainty of criminal punishment for abortions makes providers more risk averse.

While no state laws impose restrictions on birth control, the prospect of criminal liability under abortion bans adds a new uncertainty. For example, in Louisiana, one doctor prescribed Cytotec to make IUD insertion less painful. Despite birth control being completely legal, a Walgreens pharmacy refused to fill the prescription because "they could not be sure [they] weren't prescribing this for an abortion."[130] At the University of Idaho, the school's general counsel sent a memo to staff stating that employees cannot "dispens[e] drugs classified as emergency contraception by the FDA, except in the case of rape."[131] Even though contraceptives remain legal in Idaho—and protected under the Constitution—the university intended the memo to "help

127. Maria Angeles Lopez-Olivo, Harish R. Siddhanamatha, Beverley Shea, Peter Tugwell, George A. Wells & Maria E. Suarez-Almazor, *Methotrexate for Treating Rheumatoid Arthritis*, COCHRANE DATABASE SYS. REV., no. 6, 2014, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7047041/.

128. Margaret Beal & Kathy Simmonds, *Clinical Uses of Mifepristone: An Update for Women's Health Practitioners*, 47 J. MIDWIFERY & WOMEN'S HEALTH 451 (2014), https://pubmed.ncbi.nlm.nih.gov/12484667/.

129. June Seek Choi, Gideon Koren & Irena Nulman, *Pregnancy and Isotretinoin Therapy*, 185 CANADIAN MED. ASS'N J. 411 (2013), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3602257/.

130. Emily Woodruff, *As Abortion Ban Is Reinstated, Doctors Describe 'Chilling Effect' on Women's Care*, NOLA (July 10, 2022), https://www.nola.com/news/healthcare_hospitals/article_238af184-ff02-11ec-9bce-dfd660a21ce1.html.

131. Kelcie Moseley-Morris, *University of Idaho Releases Memo Warning Employees That Promoting Abortion Is Against State Law*, IDAHO CAP. SUN (Sept. 26, 2022), https://idahocapitalsun.com/2022/09/26/university-of-idaho-releases-memo-warning-employees-that-promoting-abortion-is-against-state-law/.

employees understand the legal significance and possible ramifications of the law, which includes individual criminal prosecution."[132]

Even in circumstances further removed from the pregnancy context, patients have experienced the spillover effects of abortion criminalization. In Tennessee, where it is illegal to have an abortion after six weeks of pregnancy, Becky Hubbard "decided to get sterilized so that she can go back on the only medication that has relieved her disabling pain from rheumatoid arthritis for the last eight years."[133] Her Tennessee doctor gave her an ultimatum: "if she wanted to stay on . . . methotrexate, she was told she had to go on birth control despite her age and history of infertility."[134] Because methotrexate can also end a pregnancy, doctors and pharmacists could be held criminally liable for prescribing to pregnant people.[135] Increasingly, pharmacies are changing policies to require diagnosis codes to ensure the prescription will not be used to end a pregnancy.[136] One rheumatologist described how dangerous this can be: "It becomes a huge problem if we see [a] patient on Thursday or Friday and we don't get the pharmacy to call back . . . . The patient can't get treatment for three or four days, which can be agonizing."[137]

Treatment for miscarriages post-*Dobbs* may be especially controversial since patients with miscarriage complications are often given the same medication that is used for abortions. In Washington D.C., which has among the least restrictive abortion laws in the country, Christina Zielke's ultrasound showed her fetus had no heartbeat.[138] Her doctors confirmed that she miscarried and told her the pregnancy tissue would eventually come out on its own.[139] Soon after, due to miscarriage complications she experienced excessive, life-threatening bleeding.[140] At the time, she happened to be on a trip in Ohio, where abortion was banned after six weeks of pregnancy except

132. Kelcie Moseley-Morris, *White House Calls Idaho Abortion Laws 'Extreme and Backwards' in Response to University Memo*, IDAHO CAP. SUN (Sept. 27, 2022), https://idahocapitalsun.com/2022/09/27/white-house-calls-idaho-abortion-laws-extreme-and-backwards-in-response-to-university-memo/.

133. Katie Shepherd & Frances Stead Sellers, *Abortion Bans Complicate Access to Drugs for Cancer, Arthritis, Even Ulcers*, WASH. POST (Aug. 8, 2022), https://www.washingtonpost.com/health/2022/08/08/abortion-bans-methotrexate-mifepristone-rheumatoid-arthritis/.

134. *Id.*

135. *Id.*

136. *Id.*

137. *Id.*

138. Selena Simmons-Duffin, *Her Miscarriage Left Her Bleeding Profusely. An Ohio ER Sent Her Home to Wait*, NPR (Nov. 15, 2022), https://www.npr.org/sections/health-shots/2022/11/15/1135882310/miscarriage-hemorrhage-abortion-law-ohio.

139. *Id.*

140. *Id.*

where there is a medical emergency.[141] She was bleeding profusely for hours, but Ohio doctors discharged her, saying "they needed to prove there was no fetal development."[142] Despite D.C. doctors already having diagnosed a miscarriage, Ohio doctors told her "the pregnancy could still be viable."[143] To ensure compliance with the state's abortion ban and avoid liability, Ohio doctors delayed treatment and may have endangered a patient's life.

Doctors delaying treatments and turning patients away is reminiscent of their behaviors before *Roe*, when they prioritized securing dying declarations from patients that would clear them of liability.[144] The difference now is that doctors face the added pressure of knowing every patient they see is being digitally surveilled. Doctors know that the chances of getting caught, even wrongfully, are high.

C. DATA SURVEILLANCE WILL CHILL LEGAL INFORMATION SHARING

Perhaps the most devastating chilling effect will be overdeterrence of legally seeking, sharing, and accessing information. There is evidence that censorship of abortion-related speech is already occurring, and data surveillance only exacerbates the issue.

At the University of Idaho, the same memo that cautioned staff against giving emergency contraceptives also directed staff to "avoid language that could be seen as counseling in favor of, referring for, or promoting abortion."[145] The memo was in response to Idaho's No Public Funds for Abortion Act. Since the university is public, its legal team "highly recommend[ed] employees in charge of the classroom remain neutral or risk violating this law." Even though abortion-related speech may be protected by the First Amendment,[146] professors are erring on the side of caution. One faculty member said the guidance could "cause individual faculty members, frankly, particularly those who don't have job protection like tenure, to be very, very careful. To refrain from saying things they might otherwise say[.]"[147]

141. *Id.*

142. *Id.*

143. *Id.*

144. *See supra* Section III.A.

145. Rachel Sun, *UI Employees Say Memo on Abortion, Contraception Creating Chilling Effect in Classroom*, NW PUB. BROAD. (Oct. 3, 2022), https://www.nwpb.org/2022/10/03/ui-employees-say-memo-on-abortion-contraception-creating-chilling-effect-in-classroom/.

146. Jeremy W. Peters, *First Amendment Confrontation May Loom in Post-Roe Fight*, N.Y. TIMES (June 30, 2022), https://www.nytimes.com/2022/06/29/business/media/first-amendment-roe-abortion-rights.html (presenting commentary that people have "the right, ostensibly, to talk about abortion").

147. Sun, *supra* note 145.

When *The New York Times* asked to interview a Texas doctor about patients' experiences with abortion, her hospital's public relations office asked the doctor to decline to comment. The doctor told CNN, "They're censoring me."[148] The doctor was not allowed to tell media where she works and could not communicate with journalists on her work email or using her work computer. At a different hospital, residents who posted an Instagram photo stating "Abortion is healthcare" were forced by university lawyers to take it down.[149] Perfectly legal communication about abortion—especially when housed online where law enforcement has unbridled access to it—poses too high of a risk for hospitals who fear liability.

Even though learning about abortion is completely legal, medical students and residency programs in restrictive states are discontinuing abortion training. Pamela Merritt, the executive director of Medical Students for Choice, said some medical schools are "so risk averse, they're shutting down all access. They're in a political pickle."[150] OB-GYN residency programs, which are required to provide clinical abortion experience, are facing difficulties sending residents out-of-state to get trained.[151] Since clinical capacity is limited, out-of-state programs cannot accommodate every program in an abortion-restrictive state.[152]

In addition to providers being deterred from legally sharing abortion-related information, pregnant people will also be deterred from seeking information to learn their options. Moments after *Dobbs* came down, Instagram and Facebook removed posts that offered women information about how to obtain abortion pills.[153] Nikolas Guggenberger, the executive director at the Yale Information Society Project, said that "[j]ust the possibility of using phone surveillance to enforce abortion bans will hang over the heads of people seeking abortions or helping others get them."[154] Following *Dobbs*,

148. Elizabeth Cohen, Justin Lape & Danielle Herman, *'Heartbreaking' Stories Go Untold, Doctors Say, As Employers 'Muzzle' Them in Wake of Abortion Ruling*, CNN (Oct. 12, 2022), https://www.cnn.com/2022/10/12/health/abortion-doctors-talking/index.html.

149. *Id.*

150. Olivia Goldhill, *After Dobbs, U.S. Medical Students Head Abroad for Abortion Training No Longer Provided by Their Schools*, STAT (Oct. 18, 2022), https://www.statnews.com/2022/10/18/medical-students-heading-abroad-for-abortion-training/.

151. *Id.*

152. *Id.*

153. *Instagram and Facebook Begin Removing Posts Offering Abortion Pills*, NPR (June 28, 2022), https://www.npr.org/2022/06/28/1108107718/instagram-and-facebook-begin-removing-posts-offering-abortion-pills.

154. Geoffrey A. Fowler & Tatum Hunter, *For People Seeking Abortions, Digital Privacy is Suddenly Critical*, WASH. POST (June 24, 2022), https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/.

hundreds of online posts urged women to delete their period tracking apps.[155] Even if the abortion ban does not apply to their activities, people are nonetheless deterred because they fear the mere possibility of being surveilled.

Maximal enforcement by way of maximal surveillance will result in chilling effects on legal and desirable activities such as performing a life-saving abortion, promptly treating miscarriage complications, and discussing information online. People are afraid of being placed in a situation of potential criminal liability. Their fear is reasonable—with all the possibilities data surveillance has to offer, the certainty of punishment can be extremely high.

When the enforcement mechanism of a criminal law requires us to give up digital privacy, should the law be enforced that way? How much of our legal, desirable activity are we willing to sacrifice for the enforcement of crimes? The central tension here involves the tools for administrability in one field—data surveillance in criminal law—directly threatening the values in another—control over one's information in privacy law. I argue that chilling legal abortions, legal non-abortion healthcare, and legal information sharing is too great an externality. Data surveillance must be curtailed even if that means capturing less effective enforcement of abortion bans.

V. POSSIBLE SOLUTIONS

Using data surveillance to enforce abortion bans creates too high of a privacy cost. The question becomes, who is responsible for protecting individuals' privacy? Some look to Big Tech, whose business practices create the troves of data that law enforcement exploits. But others point out that tech companies' data practices are perfectly legal, and instead argue that it is the federal government's responsibility to protect data privacy.

While tech companies do have the capability to alleviate abortion-related privacy concerns, it would be naïve to rely on their goodwill. Federal privacy legislation is necessary, but largely ineffective if it continues to allow exceptions for law enforcement's requests. Thus, I conclude that the solution is to limit law enforcement's ability to request sensitive data from Big Tech companies.

155. *See, e.g.*, Gennie Gebhart & Daly Barnett, *Should You Really Delete Your Period Tracking App?* ELEC. FRONTIER FOUND. (June 30, 2022), https://www.eff.org/deeplinks/2022/06/should-you-really-delete-your-period-tracking-app; @ECMcLaughlin, X (May 3, 2022, 10:36 AM), https://web.archive.org/web/20220504013052/https://twitter.com/ECMcLaughlin/status/1521467912162226176 ("If you are using an online period tracker or tracking your cycles through your phone, get off it and delete your data. Now.").

A. TECH COMPANIES TO THE RESCUE?

Post-*Dobbs*, tech companies have faced pressure to respond to growing concerns about data privacy.[156] Privacy experts and the general public have called on Big Tech to help women seeking abortions and have suggested a variety of rationales as to why they should do so. Privacy advocates have urged tech firms to provide better encryption, delete abortion-related data on users, and educate users about their data privacy.[157] Since tech companies hold what will be the critical evidence in abortion ban enforcement, many rightfully believe that the onus is on tech companies to stop collecting and storing this sensitive data in the first place.

Many tech companies have entered the dialogue by supporting their own employees who receive abortions, but are quieter when it comes to their data privacy practices. For example, an Apple spokesperson stated that, "[Apple] supports employees' right to make their own decision regarding their reproductive health. For more than a decade, Apple's comprehensive benefits have allowed our employees to travel out-of-state for medical care if it is unavailable in their home state."[158] Microsoft released a statement saying it "will provide travel expense reimbursement for employees seeking abortions and gender-affirming care anywhere in the country."[159] Amazon added a $4,000 employee benefit to cover out-of-state travel for reproductive healthcare or other medical issues.[160] Lyft's statement explicitly mentioned *Dobbs*: "In the wake of the Supreme Court decision on Dobbs v. Jackson Women's Health Organization, we're committed to providing team members with undisrupted access to safe and critical healthcare services."[161] A Meta spokesperson told ABC News that the company "plans to offer coverage of

156. Kimberly Adams & Jesus Alvarado, *With Roe Overturned, Tech Companies Will Have to Weigh Big Data Questions*, MARKETPLACE TECH (June 27, 2022), https://www.marketplace.org/shows/marketplace-tech/with-roe-overturned-tech-companies-will-have-to-weigh-big-data-questions/.

157. Aziz Huq & Rebecca Wexler, *Big Tech Can Help Women in a Post-Roe World. Will it?*, WASH. POST (June 1, 2022), https://www.washingtonpost.com/outlook/2022/06/01/roe-dobbs-big-tech/.

158. *Companies Respond to Abortion Ruling That Overturns Roe v. Wade*, B.C. CTR. FOR CORP. CITIZENSHIP (June 30, 2022), https://ccc.bc.edu/content/ccc/blog-home/2022/06/companies-respond-to-abortion-ruling.html.

159. *Id.*

160. *Id.*

161. *Id.*

travel expenses for some employees seeking an abortion."[162] A Google memo told employees they may relocate from states banning abortion.[163]

While Big Tech companies have shown a commitment to employees' reproductive health, their commitment to users' reproductive health remains largely opaque.[164] Many companies that released statements regarding new employee policies have declined to respond to media inquiries into their post-*Dobbs* policies and requests for data from law enforcement.[165] Huq and Wexler note that the distinction between users and employees is ultimately untenable because employees are also users whose privacy is compromised.[166]

There have been some exceptions to the general silence about abortion-related data privacy. Most notably, Google released a statement in July 2022 vowing to delete location history data from abortion clinics:

> Some of the places people visit—including medical facilities like counseling centers, domestic violence shelters, abortion clinics, fertility centers, addiction treatment facilities, weight loss clinics, cosmetic surgery clinics, and others—can be particularly personal. Today, we're announcing that if our systems identify that someone has visited one of these places, we will delete these entries from Location History soon after they visit. This change will take effect in the coming weeks.[167]

Google's decision came after Alphabet Workers Union, a minority labor union, demanded that Google delete any personal data that law enforcement could use to prosecute people who receive abortions.[168] The announcement did not make any commitments as to how Google will handle data requests from law enforcement, nor did it commit to automatically deleting search records about abortions. Instead, "[u]sers must individually opt to delete their search history."[169]

---

162. *Id.*

163. Jennifer Elias, *Google Memo on End of Roe v. Wade Says Employees May Apply to Relocate 'Without Justification,'* CNBC (June 27, 2022), https://www.cnbc.com/2022/06/24/google-memo-to-employees-on-roe-v-wade-overturn.html.

164. Huq & Wexler, *supra* note 53, at 590–91.

165. *Id.*

166. *Id.* at 592.

167. Jen Fitzpatrick, *Protecting People's Privacy on Health Topics*, GOOGLE: KEYWORD (July 1, 2022), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/.

168. Nico Grant, *Google Says It Will Delete Location Data When Users Visit Abortion Clinics*, N.Y. TIMES (July 1, 2022), https://www.nytimes.com/2022/07/01/technology/google-abortion-location-data.html.

169. *Id.*

Some privacy experts believe that the onus is on tech companies to stop collecting and storing this sensitive data in the first place.[170] However, while it is true that tech companies have the primary power to stop collecting or distributing sensitive data, I argue that we cannot rely on Big Tech to protect abortion access. First, evidence of tech companies' broken privacy promises diminishes confidence that they will live up to their policies. Second, tech companies often place the responsibility on the user to opt out of sensitive data collection, making it unlikely that unsophisticated users will do so. Finally, tech companies whose primary revenue comes from data collection cannot be left to self-regulate.

1. Evidence of Broken Privacy Promises

In 2021, the aforementioned period and ovulation tracker Flo, shared users' sensitive fertility data with third parties, in violation of its express privacy claims. Flo's privacy policy misleadingly represented that third parties could not use consumers' personal information "for any other purpose except to provide services in connection with the App."[171] However, for five years the app included tools from a variety of third-party marketing and analytics firms that gathered records of users' interactions on the app.[172] When a user entered pregnancy-related information on the app, third parties received analytics records with the word "pregnancy" attached.[173] Flo settled with the FTC over the allegations.[174] Flo agreed to notify users about how their data was shared and receive an audit of its privacy practices, but did not admit any wrongdoing.[175]

In May 2022, Twitter was fined $150 million for allegedly breaking its privacy promises. It asked users to provide their contact information to "safeguard your account," but it failed to mention that it was also used to deliver targeted ads.[176] In November 2022, Apple, who has a reputation for

170. Jordan Famularo & Richmond Wong, *How the Tech Sector Can Protect Personal Data Post-Roe*, BROOKINGS INST. (Oct. 27, 2022), https://www.brookings.edu/techstream/how-tech-firms-can-protect-personal-data-after-roe-us-privacy-abortion-surveillance/.

171. Lesley Fair, *Health App Broke Its Privacy Promises by Disclosing Intimate Details About Users*, FED. TRADE COMMISSION (Jan. 13, 2021), https://www.ftc.gov/business-guidance/blog/2021/01/health-app-broke-its-privacy-promises-disclosing-intimate-details-about-users.

172. *Id.*

173. *Id.*

174. *Id.*

175. *Id.*

176. Lesley Fair, *Twitter to Pay $150 Million Penalty for Allegedly Breaking Its Privacy Promises—Again*, FED. TRADE COMMISSION (May 25, 2022), https://www.ftc.gov/business-guidance/blog/2022/05131/twitter-pay-150-million-penalty-allegedly-breaking-its-privacy-promises-again.

strong consumer privacy protections, was sued in a class action over tracking of users' activity in violation of the California Invasion of Privacy Act.[177]

2. Placing the Responsibility on Users

The typical privacy framework for digital data processing in the United States is a "strict opt-out" option, allowing consumers to request that the company does not sell or share their personal information.[178] Tech companies place the burden on consumers to "exercise their rights and take action to prevent an organization from processing their data."[179] The opposite approach, an "opt-in" system, requires the company to affirmatively obtain consumer consent, rather than assuming it exists to begin with.[180] Notably, opt-in systems are far less common in the United States.[181]

In the current privacy framework, tech companies can "shift[] the work onto the user to figure out how to delete their data."[182] Unfortunately, just like users likely do not read terms and conditions policies, they do not typically change default data collection settings.[183] Shoshana Zuboff, a surveillance capitalism scholar, describes the power asymmetry under this framework: "Take a minute and just feel how intolerable it is for us to essentially be supplicants toward a massively wealthy, massively powerful data company, saying, 'Please, please, please stop collecting sensitive data.'"[184]

3. Clear Conflict of Interest

It is unrealistic to rely on tech companies to safeguard privacy to the necessary extent because minimizing data collection is contrary to their profit models. To ask Big Tech to solve a problem it created is to ask it to dismantle surveillance capitalism and its economic imperatives. Google is a $150 billion

177. Sarah Perez, *Apple Faces New Lawsuit Over Its Data Collection Practices in First-Party Apps, Like the App Store*, TECHCRUNCH (Nov. 14, 2022), https://techcrunch.com/2022/11/14/apple-faces-new-lawsuit-over-its-data-collection-practices-in-first-party-apps-like-the-app-store/.

178. Sarah Rippy, *Opt-in vs. Opt-out Approaches to Personal Information Processing*, INT'L ASS'N PRIVACY PROFESSIONALS (May 10, 2021), https://iapp.org/news/a/opt-in-vs-opt-out-approaches-to-personal-information-processing/.

179. *Id.*

180. *Id.*

181. *Id.*

182. Geoffrey A. Fowler, *Okay, Google: To Protect Women, Collect Less Data About Everyone*, WASH. POST (July 1, 2022), https://www.washingtonpost.com/technology/2022/07/01/google-privacy-abortion/.

183. Editorial Board, *America, Your Privacy Settings Are All Wrong*, N.Y. TIMES (Mar. 6, 2021), https://www.nytimes.com/2021/03/06/opinion/data-tech-privacy-opt-in.html.

184. Casey Newton, *Why Abortion is Tech's Next Big Reputational Risk*, KAIROS FELLOWSHIP (July 13, 2022), https://www.kairosfellows.org/news/tag/Data+Privacy.

advertising business. It was the first to create "lucrative markets to trade in human futures, what we now know as online targeted advertising, based on their predictions of which ads users would click."[185] It relies on access to users' data to develop its services and products. Sundar Pichai, Google's chief executive officer, wrote an editorial in *The New York Times* titled "Privacy Should Not Be A Luxury Good."[186] Just months later, the *Daily News* reported that unhoused people were lined up to get a $5 gift card in exchange for uploading their face scan to Google.[187] Facebook has acted similarly. In 2019, Mark Zuckerberg announced at a conference that "the future is private."[188] Just weeks later, a lawyer for Facebook argued in a user privacy case that the "very act of using Facebook negates any reasonable expectation of privacy as a matter of law."[189] Rather than relying on Big Tech's goodwill, we need strong federal privacy legislation.

B. FEDERAL PRIVACY LEGISLATION

Post-*Dobbs*, the case for federal privacy legislation is stronger than ever. As it currently stands, there are two abortion-specific data privacy bills that have recently been introduced, the My Body, My Data Act and the Health and Location Data Protection Act.

1. Overview of Proposed Federal Legislation

In June 2022, Representative Sara Jacobs introduced the My Body, My Data Act in the House. The proposed bill establishes that "commercial entities, including individuals, nonprofits, and common carriers, may not collect, retain, use, or disclose personal reproductive or sexual health information except (1) with the express written consent of the individual to whom such information relates, or (2) as is strictly necessary to provide a requested product or service."[190] The Act would also give users the right to access or delete their personal data by requiring commercial entities to "provide individuals with access to, and a reasonable mechanism to delete, any of their reproductive or

185. Shoshana Zuboff, *You Are Now Remotely Controlled*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html.

186. Sundar Pichai, *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, N.Y. TIMES (May 7, 2019), https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html.

187. Ginger Adams Otis & Nancy Dillon, *City Worker Saw Homeless People Lined Up to Get $5 Gift Card for Face Scan Uploaded to Google*, N.Y. DAILY NEWS (Jan. 31, 2020), https://www.nydailynews.com/news/national/ny-witness-saw-homeless-people-selling-face-scans-google-five-dollars-20191004-j6z2vonllnerpiuakt6wrp6l44-story.html.

188. Zuboff, *supra* note 185.

189. *Id.*

190. H.R. 8111, 116th Cong. (2022).

sexual health information upon request."[191] The bill is endorsed by Planned Parenthood, NARAL Pro-Choice America, National Abortion Federation, United for Reproductive & Gender Equity, National Partnership for Women & Families, Feminist Majority, and the Electronic Frontier Foundation.[192]

My Body, My Data is a step in the right direction to limit health-related data collection, but it likely does not do enough to prevent or mitigate law enforcement's access to and use of abortion-related data. Representative Jacobs recognized that "it's unconscionable that information could be turned over to the government or sold to the highest bidder and weaponized against us."[193] However, scholars pointed out that the Act "does not block, or indeed even mention, warrants, subpoenas, or other court orders."[194] Based on the bill's language, only collection of voluntarily shared data would be disallowed.[195] While limiting data collection in any way possible is a positive step, Representative Jacobs' bill likely does not do enough to prevent abortion criminalization via data surveillance.

Additionally, Senators Warren, Wyden, Murray, Whitehouse, and Sanders introduced the Health and Location Data Protection Act in June 2022.[196] The proposed bill bans data brokers from selling or transferring health and location data, but makes exceptions for HIPAA-compliant activities, protected First Amendment speech, and validly authorized disclosures.[197] Again, the bill falls short in specifically addressing how law enforcement can obtain abortion related data to surveil potentially pregnant people.

The Fourth Amendment Is Not For Sale Act, although not specifically about sensitive health data, does specifically address law enforcement's ability to obtain data. The bipartisan Act, introduced in 2021 by Senators Wyden, Paul, and eighteen other senators, seeks to "close the legal loophole that allows

191. *Id.*

192. Hayley Tsukayama & India McKinney, *Pass the "My Body, My Data" Act*, ELEC. FRONTIER FOUND. (June 21, 2022), https://www.eff.org/deeplinks/2022/06/pass-my-body-my-data-act.

193. SARA JACOBS, MY BODY, MY DATA ACT OF 2022, https://sarajacobs.house.gov/uploadedfiles/mybodymydataactonepager.pdf (last visited Nov. 24, 2023).

194. Huq & Wexler, *supra* note 53, at 634–35. Notably, Huq and Wexler are the first to propose creating an evidentiary privilege for abortion-relevant data. While I endorse this as an *ex-post* solution, *ex-ante* legislation is also necessary.

195. *Id.*

196. S. 4408, 117th Cong. (2022).

197. *Warren, Wyden, Murray, Whitehouse, Sanders Introduce Legislation to Ban Data Brokers from Selling Americans' Location and Health Data*, ELIZABETH WARREN (June 15, 2022), https://www.warren.senate.gov/newsroom/press-releases/warren-wyden-murray-whitehouse-sanders-introduce-legislation-to-ban-data-brokers-from-selling-americans-location-and-health-data.

data brokers to sell Americans' personal information to law enforcement and intelligence agencies without any court oversight."[198] While this would prevent the government from getting around the Fourth Amendment by simply paying for the data, police are still allowed to get a court order to compel that data.[199] This solution does not go far enough in protecting privacy, especially considering the ease with which warrants for health-related data can be obtained.

Ultimately, federal privacy legislation has much work to do. On the tech companies' side, legislation like My Body, My Data is needed to limit the information companies are allowed to collect and use. Doing so will at least limit the voluntary information collected, even if it still requires companies to disclose data to law enforcement. Data brokers selling sensitive data to law enforcement is perhaps the most obviously problematic—the Fourth Amendment Is Not For Sale Act can help reduce the amount of data law enforcement receives that is completely unregulated. Finally, even when law enforcement does have a warrant, there is a question of whether the warrant should have been granted in the first place. For data as sensitive as health information, it may be appropriate to outlaw reverse-search warrants entirely.[200]

These privacy reforms go beyond opinions on abortion constitutionality. Across party lines, Americans support federal data privacy legislation.[201] Even Republican Senator Josh Hawley, who openly rejects a constitutional right to abortions, considers data surveillance "a separate question altogether."[202] Regardless of whether abortion is a crime, there should be rights to data privacy that apply even if it makes things harder for prosecutors.

198. *Wyden, Paul and Bipartisan Members of Congress Introduce The Fourth Amendment Is Not For Sale Act*, RON WYDEN (Apr. 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-.

199. Huq & Wexler, *supra* note 53, at 635 n.355 ("the Act provides no protection against warrants or indeed against any other form of legal process applied to the majority of abortion-relevant data that does not fall within existing Fourth Amendment doctrine.").

200. Indeed, California introduced a bill to prohibit any government entity from seeking a reverse-keyword or reverse-location demand. *See* A.B. 793, 2023–2024 Reg. Sess. (Cal. 2023).

201. Chris Teale, *More Than Half of Voters Back a National Data Privacy Law*, MORNING CONSULT (Jan. 12, 2022), https://morningconsult.com/2022/01/12/federal-data-privacy-legislation-polling/.

202. Matt Laslo, *The Shaky Future of a Post-Roe Federal Privacy Law*, WIRED (Sept. 15, 2022), https://www.wired.com/story/adppa-roe-democrats-congress/.

VI. CONCLUSION

Enforcement of abortion bans post-*Dobbs* will look vastly different than they did pre-*Roe*. *Dobbs* must be considered against a backdrop of unprecedented technological advances in data surveillance that have developed since *Roe*. Modern technology allows law enforcement to achieve increasingly expansive enforcement of abortion laws. Digital data contains an enormous amount of information much about users. Search history data, location data, and even data specific to reproductive health provide a mechanism to achieve maximal enforcement of abortion laws. Our thoughts, movements, habits, and preferences are constantly tracked and sold to third parties, including law enforcement. But giving up this privacy is too high a cost. Even if it means letting some criminal abortion activity go undetected, choosing less invasive enforcement mechanisms is worth avoiding the chilling effects on legal activity.