ABORTION SURVEILLANCE AND THE DATA BROKER LOOPHOLE

Charlotte LeBarron[*]

Since Dobbs v. Jackson Women's Health Organization *imperiled abortion access across the United States, individuals are naturally more aware of the government's ability to surveil abortions via app data. There are valid privacy and morality concerns regarding the menstrual cycle and location data collected by large technology companies, particularly when it is used by criminal law enforcement to prosecute abortions. How do governments access private companies' enormous caches of sensitive data? As it turns out, when the government cannot obtain the data through traditional means like subpoenas or warrants, they can simply purchase it from a data broker instead.*

Several federal laws regulate data brokers or protect reproductive data privacy, namely, the FTC's Health Breach Notification Rule, the HIPAA Privacy Rule to Support Reproductive Health Care, and the Protecting Americans' Data from Foreign Adversaries Act. Proposed legislation like the Fourth Amendment is Not for Sale Act represents an additional attempt to remedy these issues. Additionally, a medley of state laws has sprung up, falling into three main categories: comprehensive privacy protections, data broker regulations, and reproductive health protections such as abortion "shield" laws. This Note describes how the current smattering of legislation fails to adequately prevent private entities from selling abortion app data to law enforcement.

* J.D., 2026, New York University School of Law; B.S., 2019, Boston College Carroll School of Management. Thank you to Professors Katherine Strandburg and Ignacio Cofone for their fantastic Innovation Policy Colloquium which sparked my interest in this topic. I also wish to thank the *N.Y.U. Journal of Legislation and Public Policy* staff for their incredibly thoughtful edits.

Introduction

In 2023, an Idaho teenager and his mother were charged with kidnapping for taking the teen's minor girlfriend across state lines to Oregon to have an abortion.[1] To confirm that the trio traveled to Oregon for the abortion, police used cellphone location data.[2]

1. *See A Mom and Son Are Charged in Idaho After a Teen Is Taken to Oregon for an Abortion*, NPR (Nov. 2, 2023, 2:11 PM), https://www.npr.org/2023/11/02/1210198143/idaho-abortion-kidnapping-charges-oregon-underage-girlfriend-parental-rights [https://perma.cc/JK7W-4RM7]. In Idaho, abortion is mostly banned with narrow exceptions. In Oregon, abortion is legal. *Id.*

2. *Id.*

In 2024, Senator Ron Wyden reported that an anti-abortion organization, The Veritas Society, had sent targeted misinformation to visitors of 600 abortion clinics in forty-eight states.[3] This was possible because The Veritas Society had purchased the visitors' cell phone location data from a data broker, [4] a company that is in the business of aggregating and selling consumer data.

In 2025, the Illinois Secretary of State announced that his office would investigate a suburban Chicago police department that had purchased license plate data from a private surveillance company.[5] After obtaining the data from the private surveillance firm, the police department transmitted it to a sheriff in Texas who was investigating a woman's alleged abortion in that Chicago suburb.[6]

As these examples show, state abortion shield laws and basic constitutional privacy protections are undermined by the ability of law enforcement to purchase app data from data brokers and use it in abortion investigations and prosecutions. This Note argues that closing the data broker loophole is essential to safeguarding the privacy of sensitive reproductive health decisions. Part I describes the current landscape for abortion privacy, underscoring how government-purchased information circumvents traditional legal processes for obtaining data and imperils individual privacy in a moment when reproductive rights are under attack. Part II discusses what the relevant current legal regimes do and do not achieve for reproductive health privacy. These regimes include enacted and attempted federal laws and regulations, as well as three major categories of state laws: comprehensive privacy protections, data broker regulations, and reproductive health protections

3. Press Release, Ron Wyden, U.S. Senator, Wyden Reveals Phone Data Used to Target Abortion Misinformation at Visitors to Hundreds of Reproductive Health Clinics (Feb. 13, 2024), https://www.wyden.senate.gov/news/press-releases/wyden-reveals-phone-data-used-to-target-abortion-misinformation-at-visitors-to-hundreds-of-reproductive-health-clinics [https://perma.cc/4RMX-V6ZN].

4. *Id.*

5. AP News, *Illinois Officials Investigate License-Plate Data Shared with Police Weeking Woman Who Had Abortion*, 6ABC (June 13, 2025), https://6abc.com/post/illinois-officials-investigate-license-plate-data-shared-texas-police-seeking-woman-had-abortion/16740726/ [https://perma.cc/XXJ3-CLHR].

6. *Id.* Although private surveillance firms like Flock Safety, which sold the data to the Mount Pleasant Police Department, are not exactly the same as data brokers, their function is similar. *See* Edward Vogel, *Police Surveillance Firms Are Just Data-Brokers by Another Name,* APPEAL (Feb. 1, 2023), https://theappeal.org/police-surveillance-firms-are-just-data-brokers/ [https://perma.cc/NV54-7VFJ] (noting that "while companies like ShotSpotter, license-plate-reader operator Flock Safety, and cell-phone tracker Fog Data Science pitch themselves as third-party public-safety platforms, what they really are are 'data brokers'—companies that do little other than profit by selling bulk information to others").

such as abortion "shield" laws. Finally, Part III proposes policy solutions in light of the existing gaps in the legal landscape—and argues that the best and most complete solution is a per se ban on government entities buying reproductive health data from private entities.

I. Background

A. Reproductive Rights Under Attack

Undoubtedly, *Dobbs v. Jackson Women's Health Organization* deeply complicated decisions about whether to terminate a pregnancy.[7] What once was a difficult and highly sensitive personal decision has morphed into a legal one.[8] Since *Dobbs* overturned *Roe v. Wade*, thirteen states have completely banned abortion, while six others have imposed a gestational limitation of six to twelve weeks.[9] Because many women do not even know they are pregnant at the six-week mark, these "partial" abortion bans practically operate like total bans.[10]

In some states where abortion is illegal, having an abortion can result in criminal prosecution. In the first year after *Dobbs*, 210 women faced charges for behaviors related to pregnancy, abortion, miscarriage, or birth.[11] Particularly egregious are the examples of teenagers being sentenced to jail time for having an abortion. For instance, Celeste Burgess, who had an abortion while still a minor, pled guilty to "illegally concealing or abandoning a dead body" and was sentenced by a Nebraska judge to ninety days in jail.[12] Burgess's mother, who

---

7. Dobbs v. Jackson Women's Health Org., 597 U.S. 215 (2022) (overruling Roe v. Wade, 410 U.S. 113 (1973)).

8. Of course, even before *Dobbs*, getting an abortion was not easy for many people due to state abortion restrictions—resulting in costly travel to get basic reproductive care. *See, e.g.*, Isaac Maddow-Zimmet & Kathryn Kost, *Even Before Roe Was Overturned, Nearly One in 10 People Obtaining an Abortion Traveled Across State Lines for Care*, Guttmacher (July 21, 2022), https://www.guttmacher.org/article/2022/07/even-roe-was-overturned-nearly-one-10-people-obtaining-abortion-traveled-across [https://perma.cc/9CWN-HBML].

9. *Abortion in the U.S. Dashboard*, KFF (Nov. 24, 2025), https://www.kff.org/womens-health-policy/dashboard/abortion-in-the-u-s-dashboard/ [https://perma.cc/GS7Z-UYEZ].

10. Roni Caryn Rabin, *Answers to Questions About the Texas Abortion Law*, N.Y. Times (Nov. 1, 2021), https://www.nytimes.com/2021/09/01/health/texas-abortion-law-facts.html [https://perma.cc/YEM8-VVK5] ("It is extremely possible and very common for people to get to the six-week mark and not know they are pregnant.").

11. Sarah Varney & Layla Quran, *After Roe, Pregnant Women Face Increased Risk of Criminal Prosecution*, PBS News Hour (Nov. 14, 2024, 6:30 PM), https://www.pbs.org/newshour/show/after-overturn-of-roe-more-women-face-prosecution-for-what-they-do-while-pregnant [https://perma.cc/6WU5-79AW].

12. Sanya Mansoor, *What Nebraska's Sentencing of a Teen Who Used Abortion Pills Might Mean in Post-Roe America*, Time (July 26, 2023, 4:57 PM), https://

was charged with buying Burgess abortion pills online, pled guilty to providing an illegal abortion and was sentenced to two years in prison.[13] Importantly, Nebraska law enforcement learned about Burgess's abortion through digital data—the mother and daughter discussed their plan for obtaining the abortion pills over Facebook messenger.[14]

As Celeste Burgess's story illustrates, the data used to prosecute abortions is not limited to personal health data collected by health care providers and protected by HIPAA. Rather, there is a gap between the information HIPAA might protect and the information that can be used against an individual seeking reproductive health care. In addition to medical records, information like online browsing history, unencrypted communications, location history, purchasing history, social media posts, and other app data related to health can be used to prosecute abortion.[15]

Of particular concern are period tracking apps, which collect a wide variety of data including "moods, appetite assessments, physical symptoms, and sexual intercourse."[16] These apps can serve valuable functions like helping couples who struggle with fertility issues get pregnant. However, users of cycle-tracking apps are often unaware that their personal data can be sold to third parties, including law enforcement.[17] For example, in 2021, the Federal Trade Commission ("FTC") reached a settlement with Flo Health, a menstrual cycle tracking app that the FTC had charged with sharing health data collected from their users with marketing and analytics firms, a practice inconsistent with their privacy policy. [18]

Another example is Ovia Health, a fertility tracking app where users input their basal body temperature, instances of intercourse, and

---

time.com/6298166/nebraska-abortion-pill-case-legal-experts/ [https://perma.cc/3H3J-D65M].

13. *Id.*; Mitchell McCluskey, *A Nebraska Mother Who Provided an Illegal Abortion for Her Daughter and Helped Dispose of the Fetus Gets 2 Years in Prison, Report Says*, CNN (Sep. 23, 2023, 9:30 AM), https://www.cnn.com/2023/09/23/us/nebraska-abortion-pill-jessica-burgess [https://perma.cc/Z762-J9SV].

14. Mansoor, *supra* note 12.

15. Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV. 1, 13 (2020).

16. *Id.*

17. Uma Patel et al., *Experiences of Users of Period Tracking Apps: Which App, Frequency of Use, Data Input and Output and Attitudes*, 48 REPRODUCTIVE BIOMEDICINE ONLINE 1, 6 (2024) (describing the use of period tracking apps for fertility tracking, but also the unreliability of period tracking apps for this use).

18. Press Release, Fed. Trade Comm'n, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google [https://perma.cc/ZU8N-LQC5].

cervical fluid data to receive a "fertility score."[19] Unless users read the Ovia privacy policy in detail, they are likely unaware that their health information, pregnancy status, and other sensitive, often legally protected, information can be sold "for marketing and promotion" if users "opt-in as part of a giveaway or promotion."[20] The giveaway rules are specific to each sweepstakes.[21] For example, under the "Ready, Set, Spring 2025 Official Giveaway Rules," a user who submits an entry to the contest gives "express permission" for Ovia to share their personal information with "Participating Partners."[22] It is unlikely that users entering a raffle for a bassinet or baby monitor truly understand that their fertility data, pregnancy status, and personal demographic characteristics could be transmitted to unspecified third parties.

This phenomenon is not unique to cycle-tracking apps. In 2012, Target's data-driven pregnancy prediction model figured out that a high schooler was pregnant before her parents did.[23] Using the shopper's guest ID, demographic information, and purchases of additional data about her, Target's team of marketing analysts was able to predict her pregnancy with some accuracy.[24] Notably, this was over a decade ago and long before the inception of generative AI and other machine learning models that learn from data over time, enhancing predictive accuracy.[25]

Of course, a consumer worried about surveillance of their pregnancy could simply choose not to use period tracking apps. But

19. *How to Use Your Fertility Chart*, OVIA HEALTH, https://www.oviahealth.com/guide/75/how-do-i-use-my-fertility-chart/ [https://perma.cc/3LC4-LGSR].

20. *Ovia Health by Labcorp Apps Privacy Policy*, OVIA HEALTH, https://www.oviahealth.com/privacy-policy/ [https://perma.cc/FKM2-54ZR].

21. *Giveaways*, OVIA HEALTH, https://www.oviahealth.com/giveaway/ [https://perma.cc/GRN3-8YWV] (giveaway rules are only available for sweepstakes that are currently open; a user does not need to click on the rules to enter the contest).

22. *Ovia Health's Ready, Set, Spring 2025 Official Giveaway Rules*, OVIA HEALTH, https://www.oviahealth.com/march-2025-giveaway-rules/ [https://perma.cc/76WS-A2CN] [hereinafter *Ovia Giveaway Rules*].

23. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html, [https://perma.cc/M47T-CVRC].

24. *Id.*

25. *See* Jan Stihec, *How to Use AI for Predictive Analytics and Smarter Decision Making*, SHELF (Dec. 9, 2024), https://shelf.io/blog/ai-for-predictive-analytics/ [https://perma.cc/M93Q-DH93] (describing how machine learning models can make predictions about future outcomes when confronted with new data); Kevin Beasley, *Unlocking the Power of Predictive Analytics with AI*, FORBES (Aug. 11, 2021, 8:01 AM) https://www.forbes.com/councils/forbestechcouncil/2021/08/11/unlocking-the-power-of-predictive-analytics-with-ai [https://perma.cc/KG6B-SRNN] ("Pairing predictive analytics models with AI are crucial in improving forecast accuracy . . . . An AI system could proactively flag likely events, resulting in more informed decision-making.").

even then, as research like that of Princeton professor Janet Vertesi suggests, it's quite difficult to hide a pregnancy in the information age.[26] Throughout her pregnancy, Vertesi used only cash or gift cards and avoided mentioning her pregnancy anywhere online.[27] Although she managed to go through the pregnancy without the usual bombardment of baby-related ads, her takeaway was that this approach was inadvisable, writing that, "[o]pting out makes you look like a criminal. . . . It's incredibly inconvenient. It isn't sustainable."[28]

While the Vertesi and Target examples illustrate the difficulty of hiding a pregnancy from tech companies, they happened before *Dobbs* when the stakes were lower. Now that abortion is illegal in many states, a data-driven determination that someone is pregnant does not just lead to annoying targeted ads—it can result in criminal prosecution.[29]

B. Data Brokers and the Circumvention of Traditional Legal Process

Law enforcement can obtain the digital data they use to prosecute abortions in multiple ways. First, they can use traditional means like subpoenas, court orders, and warrants.[30] Additionally, if law enforcement cannot show probable cause or otherwise fails to get digital data via these traditional measures, they can simply buy information from a data broker.[31]

1. Traditional Means of Obtaining Data

The amount of data that law enforcement requests from technology companies has been described as "staggering."[32] For instance, in the

26. Kashmir Hill, *You Can Hide Your Pregnancy Online, but You'll Feel Like a Criminal*, Forbes (Apr. 29, 2014, 8:30 AM), https://www.forbes.com/sites/kashmirhill/2014/04/29/you-can-hide-your-pregnancy-online-but-youll-feel-like-a-criminal/ [https://perma.cc/82NR-HJC2].

27. *Id.*

28. *Id.*

29. Abeer Malik, *When AI Turns Miscarriage into Murder: The Alarming Criminalization of Pregnancy in the Digital Age*, The Petrie-Flom Center (Nov. 1, 2024), https://petrieflom.law.harvard.edu/2024/11/01/when-ai-turns-miscarriage-into-murder-the-alarming-criminalization-of-pregnancy-in-the-digital-age/ [https://perma.cc/9EXS-DD75] (presenting anecdotal and empirical data to support the argument that "[t]he criminalization of pregnancy outcomes is not new, but AI introduces a high-tech dimension to an already chilling trend.").

30. Eunice Park, *Reproductive Health Care Data Free or For Sale: Post-Roe Surveillance and the 'Three Corners' of Privacy Legislation Needed*, 30 Rich. J.L. & Tech. 185, 186 (2023).

31. *Id.*

32. Ryan S. Houser, *Guarding the Sanctity of Choice and Privacy: Data Privacy and Abortion–the Next Frontier of the Fourth Amendment*, 21 Nw. J. Tech. & Intell. Prop. 201, 206 (2024).

first six months of 2024, Meta received 323,846 government requests for data and produced "some data" for 76.80% of them.[33] This number has dramatically increased over the past decade—Meta (then Facebook) first started reporting these numbers in 2013, and only about 25,600 requests were received in the first six months of that year.[34] Similarly, Google received 236,520 requests for user information in the first six months of 2024, up from 25,879 requests in the first six months of 2013.[35] As of January 1, 2024, 82% of requests to Google resulted in them providing at least some information to the government.[36] As these numbers show, government agencies obtain large amounts of digital data from technology companies, which is then often used to investigate and prosecute crimes.

These "requests" for data come in various forms. Under the Electronic Communications Privacy Act of 1986, law enforcement is limited in how it can obtain electronic data using subpoenas, court orders, or warrants.[37] The procedural requirements for each investigative tool differ, with tools requiring greater process generally providing access to more information.[38]

Subpoenas can compel disclosure of basic subscriber information including subscriber names, addresses, and telephone connection logs. There is no probable cause requirement for subpoenas,[39] but to comply with the Fourth Amendment, they must be "sufficiently limited in scope,

33. *Government Requests for User Data (Jan. 2024–June 2024)*, META TRANSPARENCY CTR., https://transparency.meta.com/reports/government-data-requests [https://perma.cc/LMD7-MPKM].

34. *Id.*

35. *Global Requests for User Information (Jan. 2024–June 2024)*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/user-data/overview?user requests=&hl=en [https://perma.cc/DQD4-YAYC].

36. *Id.*

37. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C., including 18 U.S.C. §§ 2510–23).

38. As the Department of Justice explains it, to obtain more information, law enforcement must go through more process. This means that search warrants, which enable access to more information than subpoenas or court orders, require greater process to obtain. *See* OFF. OF LEGAL EDUC., EXEC. OFF. FOR U.S. ATT'YS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 127 (2009) [hereinafter DOJ MANUAL] ("One feature of the compelled disclosure provisions of the SCA is that greater process generally includes access to information that cannot be obtained with lesser process. Thus, a []court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a []order can compel (and then some).").

39. *Id.* at 145 ("The Fourth Amendment imposes a probable cause requirement *only* on the issuance of warrants.").

relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome."[40]

Certain court orders can obtain additional personal data about subscribers, but not "the contents of communications."[41] Under Section 2703(d) of the Stored Communications Act ("SCA"),[42] court orders can be issued if the governmental entity requesting the order "offers specific and articulable facts" showing that "the records or other information sought[] are relevant and material to an ongoing criminal investigation."[43] Importantly, the government cannot merely assert that they have "specific and articulable facts" warranting a court order—they must make some showing that this is actually the case.[44]

Using a search warrant, a specific type of court order, the government can obtain everything covered by a court order plus "the *contents* of a wire or electronic communication."[45] Under the Fourth Amendment, search warrants cannot be issued without probable cause and particularity.[46] There is probable cause and particularity when "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[47]

Geofence warrants, a subset of traditional search warrants, are another mechanism law enforcement could use to investigate and prosecute abortions. Geofence warrants use location data to track the

40. See v. City of Seattle, 387 U.S. 541, 544 (1967); *see also* Wilson v. United States, 221 U.S. 361, 376 (1911) ("There is no unreasonable search and seizure when a writ, suitably specific and properly limited in its scope, calls for the production of documents which, as against their lawful owner to whom the writ is directed, the party procuring its issuance is entitled to have produced.").

41. DOJ MANUAL, *supra* note 38, at 130; 18 U.S.C. § 2703(c)(1)(B).

42. The SCA was enacted in Title II of the Electronic Communications Privacy Act of 1986. The Electronic Communications Privacy Act broadly prevents unauthorized interception or access of digital communications. The SCA includes rules for when stored communications can be disclosed. *See supra* note 37.

43. 18 U.S.C. § 2703(d) ("A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.").

44. DOJ MANUAL, *supra* note 38, at 131.

45. 18 U.S.C. § 2703(a) (emphasis added).

46. U.S. CONST. amend. IV ("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").

47. United States v. Grubbs, 547 U.S. 90, 95 (2006) (citing Illinois v. Gates, 462 U.S. 213 (1983)).

activities of people within a certain geographic area.[48] Specifically, law enforcement creates a geographic perimeter or "fence" and tracks the location data of everyone who enters this area.[49] Several states have enacted statutes protecting consumer health data from geofencing, among them Washington, Nevada, Connecticut, New York, and California.[50] Courts have, at times, expressed concerns about geofencing warrants but often uphold them.[51] In *U.S. v. Smith*, for instance, the Fifth Circuit noted that "[g]eofence warrants present the exact sort of 'general exploratory rummaging' that the Fourth Amendment was designed to prevent."[52] However, despite finding that geofence warrants violate the Fourth Amendment, the *Smith* court nonetheless denied the motion to suppress at issue given that law enforcement acted in "good faith" and with "reasonable conduct."[53] This exception for officers acting in good faith seems to be a common thread in cases involving geofences. For instance, in *U.S. v. Chatrie*, a recent Fourth Circuit case regarding geofence warrants and the Fourth Amendment, the various concurring opinions shed light on the different legal theories courts often use to uphold geofence warrants. Chief Judge Albert Diaz's concurrence agreed with upholding the geofence warrant because "the good faith exception . . . saved the warrant from suppression."[54] Judge J. Harvie Wilkinson III's concurrence, in contrast, thought there was no Fourth Amendment search. Even if there was a search, he would still uphold the geofence warrant because "there is no room for emergent judicial hostility toward this new investigative tool" given that geofences enable law enforcement to "keep pace with tech-savvy criminals."[55] In a

48. Houser, *supra* note 32, at 209.

49. Sheryl Xavier, Andrea Frey & Stephen Phillips, *Protecting Reproductive Health Data: State Laws Against Geofencing*, REUTERS (Jan. 2, 2025, 11:34 AM), https://www.reuters.com/legal/legalindustry/protecting-reproductive-health-data-state-laws-against-geofencing-2025-01-02/ [https://perma.cc/M68Z-CQQQ].

50. *Id.*

51. *See, e.g.*, United States v. Chatrie, 590 F. Supp. 3d 901, 937 (E.D. Va. 2022), *aff'd*, 136 F.4th 100 (4th Cir. 2024) (Upholding a geofence warrant under the good faith exception but noting that "[t]his Court will not simply rubber stamp geofence warrants. If the Government is to continue to employ these warrants, it must take care to establish particularized probable cause.").

52. United States v. Smith, 110 F.4th 817, 837 (5th Cir. 2024) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)).

53. *Id.* at 840 ("We hold that geofence warrants are modern-day general warrants and are unconstitutional under the Fourth Amendment. However, considering law enforcement's reasonable conduct in this case in light of the novelty of this type of warrant, we uphold the district court's determination that suppression was unwarranted under the good-faith exception.").

54. *Chatrie*, 136 F.4th at 104.

55. *Id.* at 110.

similar view, Judge Paul Niemeyer analogized electronic location data voluntarily transmitted from a crime scene to "markers" like footprints or fingerprints that traditionally fall outside the scope of a Fourth Amendment search.[56]

2. *Government Purchases of Information from Data Brokers*

If law enforcement is unable to obtain the data they need to prosecute individuals for their reproductive health choices through traditional means, they can just buy it from a data broker instead. Data brokers are companies in the business of aggregating and selling data about consumers with whom the business does not have a direct relationship.[57] They typically obtain information from publicly available sources, information-sharing agreements with apps and websites, and people's search and purchase histories.[58] In other words, when a consumer clicks "I agree" to sharing data with a website or app, this can enable the collection and transmission of their data to third parties, including law enforcement.

While the focus of this Note is abortion data, government purchases of private app data are not unique to the reproductive health context and have been happening for decades. Scholarship from the early 2000s documents "private-sector database companies that sell personal information to the government for law enforcement purposes" and proposes privacy safeguards such as minimizing the amount of personal data the government and businesses collect and applying the Privacy Act of 1974 to data brokers.[59] Later papers have commented on the "indiscriminate" nature of law enforcement's purchases of individual data from data brokers and the fact that this information has been collected in bulk.[60] In particular, Friedman and Citron have posited that, while *Dobbs* drew attention to the interconnection of private companies and the state, this problem spans beyond reproductive rights:[61]

> Today policing agencies are acquiring access to the personal data of vast swaths of society, without regard to whether the targets of data acquisition are suspected of any unlawful conduct whatsoever. And

56. *Id.* at 113.

57. Jasdev Dhaliwal, *What is a Data Broker?*, McAfee (Sept. 20, 2024), https://www.mcafee.com/blogs/tips-tricks/what-is-a-data-broker [https://perma.cc/B7HZ-F3AJ].

58. *Id.*

59. Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. Int'l L. 595, 595, 628–29 (2003).

60. Barry Friedman & Danielle Keats Citron, *Indiscriminate Data Surveillance*, 110 Va. L. Rev. 1351, 1355 (2024).

61. *Id.*

> they are using artificial-intelligence-driven tools to develop vivid pictures of who we are, what we do, where we go, what we spend, with whom we communicate, and much, much more.[62]

There are several arguments that government purchases of bulk data are beneficial or at least neutral. First, a regime that totally prevents the government from buying data while allowing private parties to obtain it could handicap law enforcement efforts.[63] However, even if law enforcement was prohibited from *buying* data, they could still get information on criminal suspects using traditional means. The benefit of making law enforcement use subpoenas, court orders, and warrants to obtain data is that these tools require process. While purchasing bulk data from a data broker makes law enforcement's job easier, this comes at the expense of individual rights.

A second argument is that government purchases of data are not unique because law enforcement often purchases tools—for instance guns and tasers—from the private sector.[64] While there might not be anything inherently wrong with the state buying the tools they need from private parties, such an argument ignores the differences in kind between a weapon and vast repositories of data. In the policing context, there are legal rules about the appropriate use of weapons.[65] The same is not true for government purchases of indiscriminate bulk data, which are, for the most part, wholly unregulated (and remain so in

62. *Id*. at 1355–56.

63. An argument sometimes made in defense of the government's purchase of data is that if private parties can buy the information, then the government should be able to as well. *See, e.g.*, Matthew Tokson, *When the Government Buys Sensitive Personal Data*, LAWFARE (Nov. 3, 2023, 9:47 AM), https://www.lawfaremedia.org/article/when-the-government-buys-sensitive-personal-data [https://perma.cc/CRY6-E4LU] (noting that "[t]he standard argument in favor of unfettered government purchases of private data is that such data is commercially available, and so anyone should be able to purchase it, including government officers"); Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants*, *Memo Says*, N.Y. TIMES (Jan. 22, 2021), http://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html [https://perma.cc/JT8L-A6K2] (noting that the Defense Intelligence Agency, a military arm of the intelligence community, does not believe a warrant is required to purchase commercially available data); *see also* Friedman & Citron, *supra* note 60, at 1357 ("Law enforcement needs to use digital tools of some sort to keep us safe from wrongdoing, and those may well require access to personal data.").

64. *See* Hoofnagle, *supra* note 59, at 597 ("After all, the private sector provides law enforcement with many tools."). For example, there is a significant industry of technology specifically sold and marketed to law enforcement. *See, e.g.*, AXON, https://taser-evolution.axon.com/ [https://perma.cc/62PL-YVVJ].

65. POLICE FOUND., READINGS ON POLICE USE OF DEADLY FORCE 65 (James J. Fyfe ed., 1982), https://www.ojp.gov/pdffiles1/87616.pdf (discussing use of deadly force rules).

most states).[66] Perhaps, with appropriate safeguards, state purchases of individual data could be justified. The current reality, however, is that many Americans lack even basic notice that their personal information is being collected, analyzed, and given to state actors.[67] Government transparency should be the procedural *floor,* and in many states even this low threshold of consumer notice is not met.[68]

3. The Constitutional Backdrop

The Fourth Amendment guarantees a right to be free from "unreasonable searches and seizures" and states that warrants shall not be issued without both "probable cause" and a particular description of "the place to be searched and the persons or things to be seized."[69] Government surveillance of personal data purchased from data brokers undermines these Fourth Amendment privacy protections.

Take the case of location data. Many apps track cell phone location.[70] Once they have location access, apps can sell this data to data brokers who repackage it and sell it to third parties including the government.[71] Data brokers often gather data from tens of thousands of apps and it can be difficult to know which apps are sharing data.[72] Some data brokers even have abortion-specific location data packages, like

66. *See infra* sections II.A & II.B.

67. Friedman & Citron, *supra* note 60, at 1371 ("Law enforcement agencies acting in coordination with private actors to gather all this information know full well that their conduct is problematic. We know that they know, because they go to great lengths to hide it.").

68. Only a handful of states have enacted data broker registration statutes that include a notice requirement. *See, e.g.*, CAL. CIV. CODE § 1798.99.82(b)(2)(E) (West 2025) (requiring data brokers to register with the California Privacy Protection Agency and disclose, among other things, "whether the data broker collects consumers' reproductive health care data"); *id.* § 1789.110 (describing consumers' right to request what information businesses are collecting about them); *id.* § 1798.99.86 (allowing consumers, through a single request, to request that every data broker that maintains any personal information delete any personal information related to that consumer held by the data broker or associated service provider or contractor).

69. U.S. CONST. amend. IV.

70. Aaron X. Sobel, *End-Running Warrants: Purchasing Data Under the Fourth Amendment and the State Action Problem*, 42 YALE L. & POL'Y REV. 176, 178 (2023) (noting that location data "is collected from virtually all applications").

71. Bennett Cyphers, *How the Federal Government Buys Out Cell Phone Location Data*, DEEPLINKS: ELEC. FRONTIER FOUND. (June 13, 2022), https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data [https://perma.cc/DK67-QQ69].

72. *Id.* (noting that a data broker called Venntel has claimed to gather data from "over 80,000" different apps).

SafeGraph's "Planned Parenthood" data package that clocks users who visit any of Planned Parenthood's United States locations.[73]

When the government buys data from a data broker to surveil citizens, this arguably violates the Fourth Amendment right to be free from "unreasonable searches and seizures." Because data is being collected on virtually *all* cell phone users, not just those suspected of crimes, the breadth and indiscriminate nature of the search almost certainly makes it "unreasonable" under the Fourth Amendment.[74] Moreover, when a government buys data from a data broker, the probable cause and particularity requirements do not apply. This evasion of traditional criminal procedure has distinct Fourth Amendment implications.

Over the last century, Fourth Amendment doctrine has evolved alongside technological advances. Specifically, the doctrine has moved toward encompassing not just searches of physical spaces, but also electronic and digital information. In 1928, *Olmstead v. United States* held that the wiretapping of defendants' residences in a conspiracy case did not amount to a search or seizure within the meaning of the Fourth Amendment because "one who installs in his house a telephone instrument with connecting wires intends to project his voice to those . . . outside."[75] This case suggested that Fourth Amendment protection did not extend to the surveillance of electronic mediums.

However, in *Katz v. United States*, the Court overturned *Olmstead*, holding that when the government electronically listens to and records a defendant's words in a public telephone booth, this constitutes a "search" that, without prior judicial authorization and safeguards, does not comply with the Fourth Amendment.[76] A new test was derived from Justice Harlan's concurrence in *Katz*: The Fourth Amendment can be invoked if there is a "legitimate expectation of privacy" established by (1) a subjective expectation of privacy and (2) the reasonableness of this expectation.[77]

---

73. Sobel, *supra* note 70, at 179.

74. In an article about indiscriminate and bulk purchases of personal data by law enforcement, the authors defined such "indiscriminate" data purchases as "acquired without the sort of lawful predicate—such as probable cause or reasonable suspicion—that typically limits when law enforcement may target individuals." Friedman & Citron, *supra* note 60, at 1355; *see also* Off. of the Dir. of Nat'l Intel., Senior Advisory Grp. Panel on Commercially Available Data, Report to the Director of National Intelligence 14 (2022) (noting that commercially available data includes "information on nearly everyone that is of a type and level of sensitivity that historically could not have been obtained").

75. Olmstead v. United States, 277 U.S. 438, 466 (1928).

76. Katz v. United States, 389 U.S. 347, 352 (1967).

77. *Id.* at 361 ("There is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that

In 2012, the Court decided *United States v. Jones*, holding that installing a GPS tracking device on an investigative target's car and using it to monitor the vehicle's movements is a "search" under the Fourth Amendment.[78] The rationale was that the Fourth Amendment guarantees the "right to be secure" in personal "effects" and the vehicle counted as such an effect.[79] *Jones* revived a "common law trespassory" test regarding what counts as a search under the Fourth Amendment.[80] Under this test, which apparently stands side-by-side *Katz*'s reasonable expectation of privacy test, a government's physical trespass into a person's property counts as "search" under the Fourth Amendment.[81] In the context of reproductive health app data, however, there is not a clear intrusion on a physical piece of property like the car in *Jones.* Thus, it is not clear that government purchases of consumer health app data would count as a "search" under the *Jones* test.

In *Riley v. California*, the Court held that a warrantless search of information on a cell phone is not generally permissible under the Fourth Amendment.[82] The court noted that cell phones differ quantitatively and qualitatively from other objects that might be kept on a person. Quantitative characteristics included phones' immense capacity for information storage, making them complete digital records of "nearly every aspect" of a life.[83] The court identified "historic location information" and "Internet search and browsing history" as qualitatively different from physical records because of their capacity to reveal granular, detailed, and sensitive information about the individual.[84] The Court concluded that, phones contain "a broad array of private information never found in a home in any form—unless the phone is."[85] In a similar Sixth Circuit case, *United States v. Warshak*, the court held that "the government may not compel a commercial [Internet Service Provider] to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause."[86]

---

society is prepared to recognize as 'reasonable.'")

78. United States v. Jones, 565 U.S. 400, 404–05 (2012).

79. *Id.* at 404 ("It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment.").

80. *Id.* at 409 ("the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test" (emphasis in original)).

81. *Id.* at 406–07.

82. Riley v. California, 573 U.S. 373, 386 (2014).

83. *Id.* at 395.

84. *Id.* at 395–96 (noting that search data can reveal a user's private concerns or neuroses and location data can reveal "specific movements down to the minute").

85. *Id.* at 396–97.

86. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010). Despite this holding, the court found no constitutional violation because agents relied on the Stored

More recently, in *Carpenter v. United States*, the Supreme Court held that individuals have a legitimate expectation of privacy regarding their physical movements that are captured by cell-site location information, so the government must generally obtain a search warrant before acquiring cell-site location information from a wireless carrier.[87] However, the *Carpenter* holding is "a narrow one" that only applies to the collection of *historical* cell-phone location data.[88] Specifically this holding did *not* extend to real-time cell-site location data and did not address "other business records that might incidentally reveal location information."[89]

Based on cases like *Warshak* and *Carpenter*, which require warrants and probable cause for cell site location information and emails from third-party Internet providers, there is an argument under the *Katz* test that consumers have a "legitimate expectation of privacy" in their personal app data. While users may have ostensibly "consented" to an app's sale of their data in some instances, the byzantine web of internet adhesion contracts and the dearth of actual consumer engagement with those contracts mean such "consent" is not truly informed.[90] Thus, under *Katz*'s "subjective expectation of privacy" prong, some consumers—even those who clicked "I agree"—subjectively believe that their data is being kept private. These users might understand that the app itself is collecting their data, without realizing that the app is then selling their personal data to third parties including law enforcement. There is also

---

Communications Act in good faith. *See id.* at 292.

87. Carpenter v. United States, 585 U.S. 296, 310–16 (2018). Cell Site Location Information is defined as "information cell phones convey to nearby towers" that "can be used to 'triangulate' a phone's location." Stephanie Lacambra, Elec. Frontier Found., Cell Phone Location Tracking or CSLI: A Guide for Criminal Defense Attorneys 1, https://www.defendyouthrights.org/wp-content/uploads/2017/10/Cell-Phone-Location-Tracking-or-CSLI-A-Guide-for-Criminal-Defense-Attorneys.pdf [https://perma.cc/ZB26-5D9R].

88. *Carpenter*, 585 U.S. at 316.

89. *Id.*; *see also* Katie Haas, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, ACLU (Mar. 27, 2014), https://www.aclu.org/news/national-security/cell-tower-dumps-another-surveillance-technique [https://perma.cc/H5JS-FZ8N] (describing "tower dumps" as a "practice of demanding an enormous amount of cell phone location information—anywhere from hundreds to hundreds of thousands of data points—in an effort to identify just a few suspects").

90. In a book chapter entitled "The Consent Illusion," Professor Ignacio Cofone argues against privacy law's reliance on "consent." He writes that because there are so many cognitive steps between the information and the risk of sharing it, consumers cannot fully understand the risk they are taking when they agree to data sharing. Thus, he concludes that "it's difficult to believe that people can ever truly make informed and welfare-enhancing decisions regarding their privacy in the information economy." Ignacio Cofone, The Privacy Fallacy: Harm and Power in the Information Economy 55 (2023).

an argument under *Katz*'s "reasonableness of expectation" prong—which is now the central inquiry— that this belief is reasonable. Given the strong ethical tradition of privacy, particularly over sensitive health information—a norm represented in the Hippocratic oath's ancient pledge and modern laws like HIPAA—it is fair to assume that Americans hold a reasonable expectation of privacy in their intimate data, especially health data. It is therefore justifiable to expect government searches of an individual's personal data to require probable cause and particularity. In short, there is a compelling argument that a "legitimate expectation of privacy" for personal app data exists under the *Katz* framework.

As the Fourth Amendment jurisprudence continues to adapt to emerging technologies, one thing is plain: The government should not be allowed to circumvent Fourth Amendment requirements for obtaining individual data by simply *buying* the information they want from a data broker. If law enforcement wants to use personal data in its investigation or prosecution of abortion, they can get a warrant. What they cannot do is buy this information from a private party in violation of the Constitution.

II. The Legal Landscape

A. Federal Laws

Several federal laws addressing data privacy rights are relevant to the problem of data brokers selling personal data to law enforcement. The FTC Health Breach Notification Rule addresses data breaches of personal health information for vendors of personal health records.[91] The HIPAA Privacy Rule to Support Reproductive Health Care imposes privacy rules on HIPAA-covered entities like health care providers and insurance companies.[92] The Fourth Amendment is Not for Sale Act, if enacted, would directly prohibit law enforcement agencies from purchasing certain personal data from data brokers.[93] Additionally, the Protecting Americans' Data from Foreign Adversaries Act prevents data brokers from transferring personal data to certain foreign powers.[94] As discussed below, each of these laws is a commendable step in the

91. FTC Health Breach Notification Rule, 16 C.F.R. § 318 (2024). Under HIPAA generally, a "health plan" means health insurance companies, HMOs, company health plans, and government plans (i.e. Medicaid). *See Covered Entities and Business Associates*, U.S. Dep't of Health & Hum. Servs., https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/VN9W-GSEP].

92. HHS HIPAA Privacy Rule to Support Reproductive Health Care, 45 C.F.R. § 164.104 (2024).

93. Fourth Amendment is Not for Sale Act, H.R. 4639, 118th Cong. (2023).

94. Protecting Americans' Data from Foreign Adversaries Act of 2024, 15 U.S.C. § 9901.

right direction. However, none of them prevent law enforcement from purchasing abortion app data from a data broker.

1. FTC Health Breach Notification Rule

In 2009, the FTC initially promulgated their Health Breach Notification Rule ("HBNR") to "strengthen privacy and security protections for health information."[95] The HBNR's purpose is to notify consumers when their personal health data is breached.[96] Essentially, if vendors of personal health records ("PHRs"), or third-party applications that store PHRs, experience a data breach, they must notify affected consumers.[97]

The HBNR applies to PHRs generally and would seemingly cover period tracker app data. However, the rule would not afford protection to internet searches or location data, which are not health records.[98] The rule would therefore not cover information like a Google search for mifepristone prescribers or GPS navigation to a Planned Parenthood.

In 2023, the FTC proposed modernizing amendments to the Health Breach Notification Rule to respond to the emergence and prominence of health apps and other direct-to-consumer health technologies.[99] In their announcing press release, the FTC mentioned recent violations of the HBNR, including actions against Premom, an ovulation tracking app that shared sensitive personal information with third parties and failed to notify consumers of these unauthorized disclosures.[100] In 2024, the FTC finalized changes to the HBNR that clarified that a "breach of security" includes third-party acquisition of identifiable health information through an unauthorized disclosure, underscored that "PHR related entities" include entities that offer products and services such as mobile applications, and expanded the relevant notice requirements.[101]

---

95. FTC Health Breach Notification Rule, 16 C.F.R. § 318 (2009).

96. Press Release, Fed. Trade Comm'n, FTC Issues Final Breach Notification Rule for Electronic Health Information (Aug. 17, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/08/ftc-issues-final-breach-notification-rule-electronic-health-information [https://perma.cc/MTD7-DVEH].

97. *Id.*

98. The HBNR covers only "personal health records" not general personal data. *See* 16 C.F.R. § 318.2. Internet searches or GPS data would not be included in the definition of "personal health records" because they are not "created or received by a . . . [c]overed health care provider . . . [h]ealth plan . . . [e]mployer . . . [or h]ealth care clearinghouse." *Id.*

99. Press Release, Fed. Trade Comm'n, FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule [https://perma.cc/W54L-2R9X].

100. *Id.*

101. Press Release, Fed. Trade Comm'n, FTC Finalizes Changes to the Health Breach Notification Rule (Apr. 26, 2024), https://www.ftc.gov/news-events/news/

Under the amended HBNR, a "[v]endor of personal health records" includes any entity—other than a HIPAA-covered entity—that is a business associate of a HIPAA-covered entity and "offers or maintains a personal health record."[102] "PHR identifiable health information" means information that relates to the past, present, or future physical or mental health of an individual and includes information that either identifies the individual or provides a "reasonable basis to believe that the information can be used to identify the individual."[103] Importantly, "breach of security" now specifies that "unauthorized disclosure" is included in the definition, which captures the sale of consumer health data to third parties.[104] Written notice under the HBNR now includes an email option for individuals who have opted in.[105] Additionally, the contents of the required notice following a breach were expanded to include steps individuals can take to protect themselves from harm and the names of any third parties who procured the data.[106]

The 2024 amendments to the HBNR help protect reproductive health data by explicitly stating that data from apps like period trackers are covered.[107] The enhanced notice requirements are also beneficial, since these allow for timely email notifications of a breach and include specific information about *which* third parties obtained *what* personal health information.

Yet, there are several ways in which reproductive health data might slip through the cracks of the HBNR. First, it includes a law enforcement exception to the "timeliness" requirements of HBNR breach notifications.[108] Generally, all notifications to individuals and the media must be sent "without unreasonable delay" and no later than sixty days after the discovery of the security breach.[109] The "Law Enforcement Exception" provides, however, that such notification will be delayed "[i]f a law enforcement official determines that a notification, notice, or posting required under this part would impede a criminal investigation."[110] This provides law enforcement with a convenient

press-releases/2024/04/ftc-finalizes-changes-health-breach-notification-rule [https://perma.cc/8SL4-C5U6] [hereinafter FTC Finalizing Press Release].

102. FTC Health Breach Notification Rule, 16 C.F.R. § 318.2.

103. *Id.*

104. *Id.*

105. *Id.* § 318.5(a)(1).

106. *Id.* § 318.6(a)–(e).

107. The fact that issuing press releases explicitly referenced a violation by ovulation tracking app, Premom, suggests these apps are covered by the new rule's amendments. *See* FTC Finalizing Press Release, *supra* note 101.

108. 16 C.F.R. § 318.4(d).

109. *Id.* § 318.4(a).

110. *Id.* § 318.4(d).

mechanism for delaying notice when they are one of the third parties who obtained the unauthorized personal health data.[111]

Another issue with the HBNR is that "unauthorized" acquisition or disclosure is not specifically defined.[112] Authorization might therefore include a consumer clicking "I agree" on a website or app's terms and conditions. Research shows that when an individual agrees to privacy policies on an app or website, they often have not read the agreement in detail.[113] One study found, for instance, that thirty-six percent of American adults say they have *never* read a privacy policy, while only thirteen percent say they read such policies "often."[114] This suggests that consent to privacy policies is rarely truly informed, even assuming the privacy policy accurately describes the company's privacy practices. Given these trends, some scholars have convincingly argued that consumer "consent" is the wrong paradigm for protecting privacy.[115] If acquiescence to privacy terms is not actually an informed choice, then individual autonomy is seemingly harmed when companies, under the guise of consent, keep sensitive information for indefinite time periods and distribute it to unspecified parties.

Further, a company might be more willing to disclose a hack than to disclose that the company intentionally allowed third-party access to individual health data. A hack, while embarrassing for the company, does not typically involve a purposeful disclosure of company data. Affirmatively selling consumer health data without adequate authorization is a greater betrayal of consumer trust and could have

111. For an examination of "law enforcement exemptions" in privacy statutes, see Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Law Enforcement Exemptions,* 111 MICH. L. REV. 485, 531 (2013). While this article does not discuss the HBNR Amendments (not yet enacted), the author notes, among other things, "[a] handful of cases—including the high profile attempt by the Department of Justice to obtain the medical records of women who received late-term abortions—have squarely confronted the conflict between HIPAA's rather broad law enforcement exemption and state confidentiality provisions" and led to "mixed results." *Id.*

112. The "definitions" provision of the HBNR does not define "unauthorized" noting only that "[u]nauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information." *See* 16 C.F.R. § 318.2.

113. Brooke Auxier et al., *Americans' Attitudes and Experiences with Privacy Policies and Laws*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/ [https://perma.cc/VQP4-A8BP] ("Just 9% of adults say they always read a company's privacy policy before agreeing to the terms and conditions.").

114. *Id.*

115. COFONE, *supra* note 90, at 46.

greater negative repercussions if disclosed. There might therefore be an incentive on the part of vendors to avoid notifying the public of such affirmative "breaches," even if they constitute an unauthorized disclosure. This could violate the HBNR, but given the current presidential administration's hostility towards the administrative state, the FTC's enforcement capabilities and priorities might not lead to any action against such violations.[116] In March 2025, the Trump Administration fired two Democratic FTC commissioners, seemingly in contravention of current constitutional removal doctrine.[117] Back in 2024, the HBNR amendments passed on a three to two vote: Recently resigned Chair Lina Khan and the two terminated Democratic commissioners voted for the amendments while the two Republican commissioners explicitly dissented.[118] Given that FTC members who opposed the HBNR remain on the Commission, enforcement of these provisions might not be a top priority for the next four years.[119] Overall, the HBNR is a laudable regulation, but it leaves gaps law enforcement could use to continue procuring individual data from third-party vendors.

2. HIPAA Privacy Rule to Support Reproductive Health Care

Under the Biden Administration, the U.S. Department of Health & Human Services ("HHS") issued a final rule modifying the HIPAA

116. A scan of the FTC's recent press releases shows that the last mention of the HBNR was Lina Khan's summary of the agency's key accomplishments, posted January 19, 2025 (the day before Trump took office). *See generally Press Releases*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/news/press-releases [https://perma.cc/X76K-XWXV].

117. David McCabe & Cecilia Kang, *Trump Fires Democrats on Federal Trade Commission*, N.Y. TIMES (Mar. 18, 2025), https://www.nytimes.com/2025/03/18/technology/trump-ftc-fires-democrats.html [https://perma.cc/42FT-ZZF7]. After the Trump administration removed FTC Commissioner Rebecca Slaughter in 2025, Slaughter sued Trump arguing that her removal was improper. *See* Slaughter v. Trump, No. 25-5261, 2025 WL 2551247 (D.C. Cir. Sep. 2, 2025), *cert. granted sub nom.* Trump v. Slaughter, --- S.Ct. ----, 222 L.Ed.2d 1233 (2025). The Supreme Court recently heard oral argument in this case, and spectators believe the Court is likely to narrow or overrule *Humphrey's Executor*, a landmark precedent establishing that the President cannot remove heads of independent federal agencies like the FTC at will. *See* Nick Bednar, *'Slaughter'-ing Humphrey's Executor*, LAWFARE (Oct. 15, 2025, 1:00PM), https://www.lawfaremedia.org/article/slaughter--ing-humphrey-s-executor [https://perma.cc/MY9B-LJMT]; *see generally* Humphrey's Ex'r v. United States, 295 U.S. 602 (1935).

118. FTC Finalizing Press Release, *supra* note 101.

119. Commissioner Holyoak left the FTC in 2025, meaning that only one commissioner (a Republican) who actually voted against the HBNR remains. Megan L. Wolf, Tiffany Aguiar & Nicholas Pung, *FTC Down to Two Commissioners After (Former) Commissioner Holyoak Leaves for U.S. Attorney Role*, CROWELL RETAIL & CONSUMER PRODS. L. OBSERVER (Nov. 20, 2025), https://www.retailconsumerproductslaw.com/2025/11/ftc-down-to-two-commissioners-after-former-commissioner-holyoak-leaves-for-u-s-attorney-role/ [https://perma.cc/7WXB-GAUG].

Privacy Rule to better protect reproductive health care privacy.[120] HIPAA is a federal law enacted in 1996 that protects sensitive patient health information from disclosure without patient consent.[121] The new rule prevents the disclosure of protected health information if the purpose is to conduct an investigation, impose liability, or attempt to identify a person "for the mere act of seeking, obtaining, providing, or facilitating reproductive health care," where such health care is "lawful" under the circumstances in which it is provided.[122] The applicable entities are health plans, health care clearinghouses, and health care providers who transmit "any health information in electronic form."[123] Protected health information ("PHI") includes demographic information that could be used to identify a person coupled with information about that person's "past, present, or future physical or mental health."[124]

An important aspect of this rule is that the prohibition on sharing PHI only applies when the reproductive health care was lawful in the state where it was provided.[125] However, there is a presumption that the reproductive health care is lawful unless the covered entity has either actual knowledge that the health care provided was illegal or a "substantial factual basis" for concluding that the specific circumstances of the reproductive health care made it unlawful.[126]

The 2024 update to the HIPAA Privacy Rule to Support Reproductive Health Care is an admirable regulation specifically focused on protecting reproductive privacy rights. However, the rule leaves several important gaps through which personal reproductive health information can still be revealed to law enforcement and other third parties.

First, the Rule—which only applies to HIPAA-covered entities like health care providers and insurance companies—does not govern tech companies or data brokers.[127] Additionally, PHI under the

120. HHS HIPAA Privacy Rule to Support Reproductive Health Care, 45 C.F.R. §§ 160, 164.

121. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CDC (Sep. 10, 2024), https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html [https://perma.cc/2CWM-XBKU].

122. 45 C.F.R. § 164.502(a)(5)(iii)(A)–(B).

123. *Id.* § 160.102.

124. *Id.* § 160.103 (definitions for "protected health information" and "individually identifiable health information").

125. *Id.* § 164.502(a)(5)(iii)(B).

126. *Id.* § 164.502(a)(5)(iii)(C).

127. *Id.* § 160.102(a) ("Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities: (1) A health plan[] (2) A health care clearinghouse [] (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.").

HIPAA Privacy Rule includes only health information.[128] Given these characteristics, much of the app data this paper has focused on would not be captured by the prohibition. For instance, the SafeGraph package showing individuals who visited Planned Parenthood locations would not be regulated under the HIPAA Privacy Rule given that SafeGraph is not a HIPAA-covered entity.[129] Additionally, the location data provided by SafeGraph might not be considered PHI under the rule. One could argue that visiting an abortion clinic "relates to the provision of health care to an individual" under the definition of "individually identifiable health data."[130] However, the Rule does not explicitly mention location data, suggesting it might not be covered.

Additionally, the law provides a specific exception for reproductive health care provided unlawfully. This could create thorny issues. For instance, imagine that an abortion seeker lives in a state where abortion is illegal. They get a prescription for mifepristone from a provider in a state where abortion is legal. Is this "lawful under the law of the state in which such health care is provided under the circumstances in which it is provided?"[131] This would likely depend on the specific state laws.

While the HIPAA Privacy Rule presumes reproductive health care is lawful,[132] rebutting the presumption might not be very difficult. For instance, if law enforcement has some limited information that an abortion occurred, they could seemingly provide it to HIPAA-covered entities to rebut the presumption. Beyond requesting data from HIPAA-covered entities, law enforcement can still buy app data from data brokers. On the flip side, this standard might at least prevent law enforcement from requesting personal reproductive health information from HIPAA-covered entities in *bulk* since there is a specificity requirement.[133] Overall, although the lawfulness provision of the Rule is seemingly crafted to protect the privacy rights of abortion seekers, it might still result in HIPAA-covered entities disclosing to law enforcement the reproductive health data of individuals in states where abortion is illegal.

---

128. *Id.* § 160.103 ("Protected health information means individually identifiable *health information*: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium." (emphasis added)).

129. The only covered entities are health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form. *Id.* § 160.102(a). SafeGraph is none of these.

130. *Id.* § 160.103.

131. *Id.* § 164.502(a)(5)(iii)(B).

132. *Id.* § 164.502(a)(5)(iii)(C).

133. *Id.* § 164.512(f)(1)(ii)(C)(2).

Further, it is not clear whether the HIPAA Privacy Rule to Support Reproductive Health Care will hold up in court, as it is currently facing a legal challenge in Texas. In *Purl v. HHS*, a doctor and medical clinic sued HHS arguing that the Rule was arbitrary and capricious and exceeded HHS's authority under the Administrative Procedure Act.[134] Judge Matthew Kacsmaryk in the Northern District of Texas issued a preliminary injunction in the case, preventing HHS from enforcing the HIPAA Privacy Rule against the plaintiffs.[135] Judge Kacsmaryk also ordered the parties to provide additional briefing on how (1) *Loper Bright v. Raimondo*, (2) the major questions doctrine, and (3) the nondelegation doctrine "affect the constitutionality or legality of HIPAA *and* HHS's authority to issue the 2024 Rule."[136]

3. The Fourth Amendment is Not for Sale Act

In 2023, the Fourth Amendment is Not for Sale Act was introduced in the U.S. House of Representatives.[137] If enacted, this law would amend the SCA to prohibit law enforcement from purchasing personal data in stored electronic communications from data brokers. The SCA already prevents certain technology providers from disclosing the contents of stored electronic communications to third parties; the Fourth Amendment is Not for Sale Act would extend that prohibition to data brokers.[138]

At first glance, it might seem that this proposed law would completely fix the data broker issue in the reproductive health context. However, this is not the case. The SCA only pertains to data stored by Internet Service Providers. There are two main types of data covered by the SCA: Electronic Communications Services ("ECS") and Remote Computing Services ("RCS"). ECS providers are cell phone providers, email providers, and social media platforms meaning that emails,

134. Purl v. U.S. Dep't of Health & Hum. Servs., 760 F. Supp. 3d 489, 496 (N.D. Tex. 2024).

135. The court concluded that a preliminary injunction was warranted given the irreparable harm to Plaintiffs of financial compliance costs, Plaintiffs' likelihood of success on the merits, and a "balance of equities and public interest" that tipped towards Plaintiffs given child abuse reporting requirements that would apparently conflict with the HIPAA Privacy Rule. *Id.* at 498–99, 503–04.

136. *Id.* at 505.

137. Fourth Amendment is Not for Sale Act, H.R. 4639, 118th Cong. (2023).

138. *Id.* ("A law enforcement agency of a governmental entity and an element of the intelligence community may not obtain from a third party in exchange for anything of value a covered customer or subscriber record or any illegitimately obtained information.").

text messages, and social media messages would be covered.[139] RCS providers offer computer and cloud storage, capturing communications like photos, videos, and documents stored on a cloud-based service like Dropbox.[140] Importantly, the SCA does *not* cover many other types of apps that collect and store personal information.[141] Thus, even if data brokers were precluded from selling information covered by the SCA to third parties, this would not include certain data like health information in a period tracking app since this is not a covered communication. In sum, a much broader law, encompassing the full breadth of app and online data that could incriminate abortion seekers, is needed to close the data broker loophole in the abortion context.

4. Protecting Americans' Data from Foreign Adversaries Act

In 2024, Congress enacted the Protecting Americans' Data from Foreign Adversaries Act.[142] Enforced by the FTC, this law makes it illegal for a data broker to "sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual" to foreign adversaries.[143] Because this law only covers the sale of data to foreign powers, it is irrelevant to the sale of individual abortion data to American law enforcement. However, the law does suggest that while lawmakers are aware of the potential for misuse of sensitive individual data held by data brokers, they have elected to leave this dangerous dynamic unchecked in the domestic context.

B. State Laws

In addition to the federal regulations and legislation described above, state laws address the issue of reproductive health privacy and government purchase of personal information from data brokers. These laws fall into three main categories: comprehensive privacy laws, data broker regulation laws, and privacy legislation specific to reproductive health, such as abortion shield laws.

---

139. Jimmy Balser, Cong. Rsch. Serv., LSB10801, Overview of Governmental Action Under the Stored Communications Act (SCA) 2 (2022).
140. *Id.*
141. Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*, Brennan Ctr. for Justice (Feb. 13, 2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole [https://perma.cc/NHK9-XJBU].
142. Protecting Americans' Data from Foreign Adversaries Act of 2024, 15 U.S.C. § 9901.
143. *Id.* § 9901(a).

1. Comprehensive Privacy Laws

Currently, around twenty states have comprehensive privacy laws.[144] A law is considered comprehensive if it governs consumer data privacy generally, rather than covering a specific subset of data types.[145] This section will discuss the comprehensive privacy regimes in the first three states to enact such laws: California, Virginia, and Colorado.

California Consumer Privacy Act of 2018

California is at the forefront of state comprehensive privacy law, having enacted its trendsetter legal regime, the California Consumer Privacy Act ("CCPA"), in 2018.[146] The CCPA gives citizens of California the right to obtain information from businesses about how their personal information is being collected, used, and retained.[147] In 2020, California approved Proposition 24, the California Privacy Rights Act ("CPRA"), which amended the CCPA to add additional consumer privacy rights and business obligations.[148] Under these laws, the rights of California consumers include limiting the use and disclosure of their sensitive personal information, a right to opt out of the sale of their personal information, a right to correct inaccurate personal information, a right to know which personal information businesses have collected, and a right to delete personal information that businesses have collected.[149]

The CCPA's deletion right is expansive, allowing consumers to request that a business delete "any personal information" it might have collected about them.[150] Personal information includes demographic and biometric information, internet history, geolocation data, sensitive personal information, and "[i]nferences drawn from any of the information identified in this subdivision to create a profile

144. *Which States Have Consumer Data Privacy Laws?*, Bloomberg L. (April 7, 2025), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#map-of-state-privacy-laws [https://perma.cc/74JU-468V].

145. *See* Andrew Folks, *Defining 'Comprehensive': Florida, Washington and the Scope of State Tracking*, IAPP (Feb. 22, 2024), https://iapp.org/news/a/defining-comprehensive-florida-washington-and-the-scope-of-state-tracking/ [https://perma.cc/UC9J-P3SW].

146. Cal. Civ. Code § 1798.100 (West 2025); *see also Frequently Asked Questions: General Information About the CCPA*, Cal. Priv. Prot. Agency, https://cppa.ca.gov/faq.html [https://perma.cc/P2Q2-5H4X] (noting that the CCPA was signed into law in 2018 and became effective in 2020).

147. *See Frequently Asked Questions: General Information About the CCPA*, *supra* note 146.

148. *Id.* The CPRA amendments went into effect on Jan. 1, 2023. *Id.*

149. Cal. Civ. Code §§ 1798.105, .106, .110, .115, .120, .121, .130 (West 2025).

150. *Id.* § 1798.105(a).

about a consumer."[151] Personal information does not, however, include information that is publicly available, is deidentified, or is part of aggregated consumer information.[152]

Notably, "sensitive personal information" includes personal information concerning a "consumer's precise geolocation," personal information "collected and analyzed concerning a consumer's health," and personal information related to a consumer's "sex life."[153] Although the CCPA does not mention reproductive health directly, these categories of "sensitive personal information" could help individuals keep data around abortion decisions private.

Importantly, the CCPA's deletion provision goes beyond mere notice, giving consumers an actual mechanism to purge their data from unwanted business repositories. However, there are potential technological issues with deletion of personal data when it comes to generative AI ("GenAI"). As A. Feder Cooper and his co-authors point out in recent scholarship, deleting information that has already been fed into a GenAI algorithm is not as simple as deleting information from a traditional consumer database.[154] The GenAI deletion process, dubbed "machine unlearning," might not completely eliminate consumer information from a GenAI model even if the model is retrained from scratch without the data (a very time intensive process).[155] Specifically, these scholars argue that latent data—that is, data that are not explicitly presented to the model during training—can sometimes still be "derived or otherwise elicited from a trained model based on the patterns that the model has learned during training."[156] If true, the retention of latent data seriously complicates the CCPA deletion right: Consumers have a right to delete "inferences" based on their personal data, but this might not be technologically possible in the GenAI context. Retention of latent data could also mean that state regulatory bodies will struggle to ensure that tech companies actually delete consumer data once the deletion right has been exercised.

Another limitation of the CCPA is that only California residents have a privacy right under the statute.[157] Abortion is legal in California,

151. *Id.* § 1798.140(v)(1).
152. *Id.* § 1798.140(v)(2)(A), (3).
153. *Id.* § 1798.140(ae) (defining "sensitive personal information").
154. A. Feder Cooper et al., *Machine Unlearning Doesn't Do What You Think: Lessons for Generative AI Policy, Research, and Practice* 2 (Stanford Pub. L. Working Paper, 2025).
155. *Id.*
156. *Id.* at 7, 29.
157. *See Frequently Asked Questions: General Information About the CCPA*, *supra* note 146.

so abortion seekers might travel there to access reproductive health care. For such non-residents, the CCPA rights, including deletion, would not be available.

Additionally, several of the CCPA provisions—like the consumer right to prevent the sale or sharing of one's personal information—are "opt-out," placing the onus on consumers to act.[158] Requiring consumer action could be an issue given what scholars have dubbed "the privacy paradox": Although consumers claim to value privacy highly, they often make choices that are not conducive to privacy.[159] Empirical studies indicate that while users express concerns about the handling of their personal data, most of them voluntarily give away this same personal data by posting on social media, using fitness trackers, or enabling cookies.[160] There are several potential explanations for these findings. Maybe consumers simply do not care *that* much about privacy and thus regulation should not intervene. Or perhaps they reflect a gap in knowledge—the most vulnerable consumers might also be those with the least awareness of both what is happening to their data and their opt-out right.[161] In the abortion context, individuals from less privileged socioeconomic or educational backgrounds might be the ones struggling

158. Under the CCPA, consumers have a "right to *request* that a business delete any personal information." CAL. CIV. CODE § 1798.105(a) (emphasis added). In other words, they must affirmatively opt out of their data being stored. *See also* Sarah Rippy, *Opt-In vs. Opt-Out Approaches to Personal Information Processing*, IAPP (May 10, 2021), https://iapp.org/news/a/opt-in-vs-opt-out-approaches-to-personal-information-processing [https://perma.cc/FEE7-KHFJ] (noting that in a typical opt-out scenario the "burden is on adult consumers to exercise their rights and take action to prevent an organization from processing their data.").

159. *See* Spyros Kokolakis, *Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon*, 64 COMPUTS. & SEC. 122, 122 (2017) ("Anecdotal and empirical evidence indicate that individuals are willing to trade their personal information for relatively small rewards. . . . This dichotomy of information privacy attitude and actual behaviour has been coined the term 'privacy paradox.'").

160. *See* Nina Gerber et al., *Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior*, 77 COMPUTS. & SEC. 226, 227 (2018) ("On the one hand, users express concerns about the handling of their personal data and report a desire to protect their data, whereas at the same time, they not only voluntarily give away these personal data by posting details of their private life in social networks or using fitness trackers and online shopping websites which include profiling functions, but also rarely make an effort to protect their data actively, for example through the deletion of cookies on a regular basis or the encryption of their e-mail communication.").

161. *See, e.g.*, Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1072–73 (1999) (arguing that "[s]ome consumers [who do not want to receive solicitations] do not take advantage of opt-out lists because they may not know about them. . . . [M]any consumers remain largely unaware of how businesses use their personal information.").

to access reproductive health care, the ones unaware of how their data is being used, and the ones least likely to take the time to opt out of data sharing. Thus, an opt-out right might not fully protect these vulnerable individuals.

Virginia and Colorado

Virginia and Colorado were also early adopters of comprehensive privacy laws. In 2021, Virginia became the second state to pass comprehensive data privacy protection upon enacting the Virginia Consumer Data Protection Act ("VCDPA").[162] Similar to the California regime, Virginia gives state citizens the right to obtain information about personal data collected by businesses and request that this data be deleted.[163] Like California, consumers can also opt out of the processing of their personal data for targeted advertising, sale, or "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer."[164] Data controllers must limit the collection of personal data to what is adequate, relevant, and reasonably necessary given the purpose for which the data was collected.[165] They must also clearly disclose the categories of third parties with whom the controller shares personal data and provide consumers with clear information on how to opt out of data processing.[166] Unlike California, there is no state privacy agency specifically designated to enforce the VCDPA, which is instead handled by the Virginia Attorney General.[167]

Following suit, Colorado adopted the Colorado Privacy Act ("CPA") in 2021.[168] The CPA involves five main rights for citizens of Colorado: a right to access, a right to correction, a right to delete, a right to data portability, and a right to opt out.[169] Like Virginia, the state attorney general and district attorneys have enforcement authority.[170]

Overall, privacy rights under the VCDPA and CPA are akin to those under the trendsetter California law. These laws are a step toward giving consumers more autonomy over their personal data—including data that could be used to prosecute abortions. However, as discussed above, these comprehensive privacy laws might have technological

162. *Which States Have Consumer Data Privacy Laws?*, *supra* note 144.
163. VA. CODE ANN. § 59.1-577 (West 2025).
164. *Id.*
165. *Id.* § 59.1-578(A)(1).
166. *Id.* § 59.1-578(C)(4)–(5), (D).
167. *Id.* § 59.1-584(A).
168. *Which States Have Consumer Data Privacy Laws?*, *supra* note 144.
169. COLO. REV. STAT. ANN. § 6-1-1306(1) (West 2025).
170. *Id.* § 6-1-1311(1)(a).

feasibility issues, and their opt-out provisions might not fully protect vulnerable consumers.

2. *Data Broker Regulation Laws*

Five states—California, Nevada, Oregon, Texas, and Vermont—have also adopted laws regulating data brokers. These laws take various forms. For instance, California includes a robust data deletion right for consumers, while other states merely create a data broker registration system. The California and Nevada laws mention reproductive health data explicitly, while other states' do not.

California

Once again, California is at the forefront of data privacy legislation. The state's "Delete Act" requires data brokers to register with the California Privacy Protection Agency ("CPPA"), pay a registration fee, and catalog the types of information they collect.[171] Specifically, data brokers must disclose whether they collect the personal information of minors, consumers' precise geolocation, and, importantly, consumers' reproductive health care data.[172] Data brokers must also provide consumers a link to their website describing how consumers can delete personal information, correct inaccurate personal information, learn what information is collected about them, opt out of the sale or sharing of personal information, or learn how to limit the use and disclosure of sensitive personal information.[173] "Personal information" and "sensitive personal information" have the same definitions as the CCPA.[174]

The CPPA is also tasked with establishing an "accessible deletion mechanism."[175] This deletion mechanism would allow a consumer—through a single, free request—to demand that every data broker maintaining their personal information delete it.[176] Data brokers must establish a deletion mechanism by January 1, 2026.[177] It thus remains to be seen how effective the CPPA is in ensuring that consumer data is actually deleted by companies once the deletion right is exercised.

171. Cal. Civ. Code § 1798.99.82 (West 2025).
172. *Id.* § 1798.99.82(b)(2)(C)–(E).
173. *Id.* § 1798.99.82(b)(2)(g).
174. *See supra* notes 150–53.
175. Cal. Civ. Code § 1798.99.86(a).
176. *Id.* § 1798.99.86(b).
177. *Id.* § 1798.99.86(a).

Nevada

In Nevada, operators of websites that collect personal information from consumers must notify consumers that their information is being collected. Consumers can also submit a request to these website operators or data brokers asking them not to sell the consumers' personal information.[178]

Nevada's general data broker regulation does not include a deletion provision. However, there is an exception for consumer health data (including reproductive or sexual health care),[179] which consumers can request that the regulated entities delete.[180] The unauthorized sale or offering of consumer health data is prohibited, as is geofencing within 1,750 feet of a medical facility for the purpose of identifying or tracking consumers seeking health care.[181]

Oregon

In Oregon, a 2023 law requires that data brokers register with Oregon's Department of Consumer and Business Services if they collect, sell, or license brokered personal data.[182] The definition of "brokered personal data" does not explicitly reference reproductive health information, though it does include an expansive catch-all provision for "[o]ther information that, alone or in combination with other information that is sold or licensed, can reasonably be associated with the resident individual."[183]

Seemingly, the Oregon law imposes weaker requirements on data brokers than Nevada or California. Data brokers are not *required* to allow individuals an opt-out right to the collection, sale, or licensing of their brokered personal data—the data broker simply must *state whether* they offer such a right.[184] However, this notice is provided to the Department of Consumer and Business Services, not to consumers.[185] The law also does not explicitly call for establishing a public listing of data brokers or provide a deletion right.

178. Nev. Rev. Stat. Ann. § 603A.345 (West 2025).
179. *Id.* § 603A.430 (defining "consumer health data").
180. *Id.* § 603A.505(a).
181. *Id.* § 603A.540(2)(b).
182. Or. Rev. Stat. Ann. § 646A.593(2)(a) (West 2025).
183. *Id.* § 646A.593(1)(a)(G).
184. *Id.* § 646A.593(3)(c).
185. *Id.*

Texas

Texas's data broker regulation requires that data brokers post a conspicuous notice on their website or app stating that the entity maintaining the site is a data broker.[186] Additionally, data brokers must register with the Texas Secretary of State and disclose, among other things, the types of data they collect and transfer.[187] This registration information will be used to construct a searchable database of data brokers operating in the state.[188] Data brokers are also required to develop comprehensive security measures to protect the consumer data they hold.[189]

Reproductive health data is not included in the definition of "sensitive data," although this definition does include precise geolocation data, "information that describes or reveals an individual's . . . health diagnosis, condition, or treatment," and some private communications on personal devices.[190]

Vermont

In Vermont, data brokers must register with the Secretary of State and provide information about the data broker's practice.[191] In particular, the data brokers must disclose whether or not they allow consumers to opt out of personal data collection or sale.[192] If consumers cannot opt out of particular data collection, databases, or sales activities, this must be disclosed to the Secretary as well.[193]

Vermont also requires data brokers to create a comprehensive information security program to protect personally identifiable information. These controls must have administrative, technical, and physical safeguards appropriately calibrated to the circumstances of the data broker.[194]

***

State-level data broker registries are a great first step in regulating data brokers, but they are just that—a first step. In theory, searchable registries of regulated entities could be beneficial. However, such benefits will only accrue if consumers can *access* and *use* the

186. Tex. Bus. & Com. Code Ann. § 510.004 (West 2025).
187. *Id.* § 510.005.
188. *Id.* § 510.006.
189. *Id.* § 510.007.
190. *Id.* § 510.001(15).
191. Vt. Stat. Ann. tit. 9, § 2446(a) (2025).
192. *Id.* § 2446(a)(3)(B).
193. *Id.* § 2446(a)(3)(C).
194. *Id.* § 2447(a)(1).

information. For instance, FINRA's BrokerCheck website enables individuals to easily search for a financial advisor's misconduct history, but a 2019 study found that only seven percent of investors surveyed used the tool.[195] Unsophisticated consumers are probably similarly unlikely to look up a specific data broker on a state website. If true, consumer inaction would limit the usefulness of these data broker registries. Additionally, many of the state laws stop at notice and registration, lacking the opt-out and deletion consumer rights present in the California Delete Act.[196] While it is a good starting point for state governments to have a list of data brokers, mere registration with no opt-out or deletion right does little to protect consumers from inappropriate data collection.

Some of the state laws, such as the Texas statute, exclude deidentified data from the "personal data" definition.[197] Although this seems sensical on its face, research suggests that deidentified data can be re-identified when datasets are combined, whether or not re-identification is the intent.[198] Re-identification risk seems to be relatively low—one study estimated it at one percent[199]—although it is possible that GenAI will make it easier to piece together inferences about deidentified data.

Overall, while the spirit of these data broker regulation laws is commendable, it is not clear that they will be effective. Of these laws, California and Nevada seem to provide the most protection to consumers since they go beyond notice and registration and require data brokers to give consumers opt-out rights. The general deletion right in California is the most protective, as it affords a mechanism for consumers to claw back their data from data brokers entirely.

3. Laws That Protect Reproductive Health Data Specifically

Some states also have laws safeguarding reproductive health data specifically. Abortion shield laws, which protect abortion seekers and

195. FINRA is a self-regulatory body overseeing U.S. broker-dealer firms. *See BrokerCheck*, FINRA, https://brokercheck.finra.org/ [https://perma.cc/Y8Y7-J9ZU]; JUDY T. LIN ET AL., FINRA INV. EDUC. FOUND., INVESTORS IN THE UNITED STATES: A REPORT OF THE NATIONAL FINANCIAL CAPABILITY STUDY 1 (2019).

196. *See, e.g.*, OR. REV. STAT. ANN. § 646A.593 (West 2025).

197. TEX. BUS. & COM. CODE ANN. § 510.001(11) (West 2025).

198. SPRINGER, PRIVACY AND DATA PROTECTION IN SOFTWARE SERVICES 51 (Roberto Senigaglia et al. eds., 2022) ("[A]n entity may have access to a dataset that at face value is anonymous but might then, purposefully or not, subsequently gain access to a dataset containing information that enables re-identification.").

199. CJ Carey et al., *Measuring Re-Identification Risk*, 1 PROC. ACM MANAG. DATA 1, 3 (2023).

providers from various out-of-state legal consequences, including but not limited to improper use of their data, are one type of law that falls into this category. Around eighteen states have abortion shield laws, which often apply when patients from an anti-abortion state obtain care in a state where abortion is legal.[200] The following is not a comprehensive list of such laws; the states included merely represent a sampling of robust or otherwise noteworthy state-level laws passed in the last few years.[201]

Washington

In 2023, Washington passed the My Health My Data Act ("MHMDA"), which, along with its Shield Law, works to keep reproductive health data private and shield providers and patients from criminalization in other states.[202] The MHMDA provides that businesses operating in Washington must maintain a clear consumer health data privacy policy disclosing the types of data collected and their uses.[203] Regulated entities may not collect or share consumer health data (which includes "[r]eproductive or sexual health information") without consumer consent.[204] Under the MHMDA, consumers have a right to find out whether regulated entities are collecting, sharing, or selling their health data and to obtain a list of third parties and affiliates who have the data.[205] There is also a deletion right and a prohibition on geofencing around entities that provide in-person health care services.[206]

The MHMDA's conception of consent is relatively robust compared to other data privacy laws. "Consent" cannot be obtained through a "terms of use agreement or a similar document that contains descriptions of personal data processing along with other unrelated

200. *Interstate Shield Laws*, Ctr. for Reprod. Rts. (June 26, 2024), https://reproductiverights.org/interstate-shield-laws/ [https://perma.cc/R3MW-B8PF].

201. *See* Kate Black et al., *The State of US Reproductive Privacy in 2025: Trends and Operational Considerations*, IAPP (Jan. 30, 2025), https://iapp.org/news/a/the-state-of-us-reproductive-privacy-in-2025-trends-and-operational-considerations [https://perma.cc/WK8F-6MCQ] ("The most prominent post-*Dobbs* health privacy framework is Washington state's My Health, My Data Act, which took full effect last year. The MHMDA establishes a novel framework to regulate the collection, processing and transfer of consumer health data, a term the law defines to include a broad range of personal information, including information that has not traditionally been treated as health data under the law.").

202. Wash. Rev. Code Ann. §§ 19.373.005–.900 (West 2024).

203. *Id.* § 19.373.020.

204. *Id.* §§ 19.373.010(8)(b)(viii), .030.

205. *Id.* § 19.373.040.

206. *Id.* §§ 19.373.040(1)(c), .080.

information" and cannot be obtained through deceptive web designs.[207] Additionally, the MHMDA sets the most protective default rule: It is unlawful for anyone to sell consumer data without *first* obtaining valid authorization.[208] In other words, a consumer must opt in to the sale of their data. Valid authorization is again relatively robust since consumers are entitled to the identity and contact information of the buyer and seller of the data, a description of the specific data being sold, a statement that the consumer can revoke their authorization at any time, and a one-year expiration date on the agreement.[209] These provisions require an active process for consumers to affirmatively opt in to the sale of their consumer health data. In particular, the one-year expiration gives consumers multiple chances to review whether they would prefer to keep the specified data private.

Washington also passed an abortion shield law in 2023.[210] This law prevents out-of-state governments from subpoenaing information about the provision or receipt of "protected health care services" in Washington. These protected health care services explicitly include abortion. Courts are also prevented from issuing orders to intercept communication if the purpose is to investigate potential criminal liability for providing, assisting, or receiving an abortion. Further, the governor of Washington will not surrender individuals charged by another state with providing, receiving, or assisting in an abortion. The shield law and MHMDA complement each other: The shield law attempts to prevent out-of-state actors from *subpoenaing* reproductive health data, while the MHMDA attempts to prevent the *sale* of reproductive health data. While data brokers are not mentioned specifically in either law, they are perhaps captured in the definition of "regulated entity" under the MHMDA, which includes a legal entity that "produces or provides products or services that are targeted to consumers in Washington" and that "determines the purpose and means of collecting, processing, sharing, or selling of consumer health data."[211]

New York

New York has also recently adopted several laws designed specifically to protect reproductive health data. Senate Bill 36A provides that the prescription label for mifepristone, misoprostol, and

207. *Id.* § 19.373.010(6).
208. *Id.* § 19.373.070(1).
209. *Id.* § 19.373.070(2).
210. *Id.* §§ 7.115.010–.020.
211. *Id.* § 19.373.010(23).

other abortion-inducing drugs can exclude the name of the prescriber.[212] This simple yet important law, an expansion of New York's existing shield laws, will help New York abortion providers avoid prosecution for prescribing abortion pills to citizens of states where abortion is illegal. The bill came as a direct response to cases like that of Dr. Margaret Carpenter, a New York doctor charged with a felony in Louisiana for allegedly prescribing abortion pills to a pregnant minor.[213] Dr. Carpenter's case remains unresolved, but New York, per their shield law, notably refused to extradite Dr. Carpenter to Louisiana.[214]

Since abortion shield laws are relatively new, it is unclear how exactly they'll hold up in courts. However, answers might be coming soon: In March 2025, a New York county clerk blocked Texas from filing a separate civil action against Dr. Carpenter.[215] To pursue the suit further, Texas would likely need to file a suit in New York state or federal court.[216]

Additionally, the New York Legislature recently advanced a health information privacy bill, Senate Bill 929, that was ultimately vetoed by Governor Kathy Hochul in December 2025.[217] This law would have generally required regulated entities to get consent before selling an individual's health information.[218] According to the bill, valid consumer authorization must include the "circumstances under which the entity may disclose regulated health information to law enforcement."[219] The bill would have also provided for an

212. N.Y. Educ. Law § 6810(1-a) (McKinney 2025).

213. Jamie Stengle, *New York Doctor Is Fined in Texas, Charged in Louisiana Over Abortion Pills in Tests of Shield Laws*, Associated Press (Feb. 14, 2025, 5:57 PM), https://apnews.com/article/abortion-doctor-maggie-carpenter-pills-847112cde026e29333c3481310593582 [https://perma.cc/D89S-CZXY].

214. Rosemary Westwood, *After Historic Indictment, Doctors Will Keep Mailing Abortion Pills over State Lines*, NPR (Mar. 19, 2025, 5:00 AM), https://www.npr.org/sections/shots-health-news/2025/03/19/nx-s1-5312115/margaret-carpenter-indictment-telemedicine-abortion-louisiana-mail-mifepristone-misoprostol [https://perma.cc/CFN7-TPJJ].

215. Pam Belluck, *New York County Clerk Blocks Texas Court Filing Against Doctor over Abortion Pills*, N.Y. Times (Mar. 27, 2025), https://www.nytimes.com/2025/03/27/health/new-york-texas-abortion-shield-law.html [https://perma.cc/ABT6-KL6S].

216. *Id.*

217. For a response to this veto, see Press Release, Liz Kreuger, New York Senator, Statement from Senator Liz Krueger and Assembly Member Linda Rosenthal on Governor's Veto of New York Health Information Privacy Act (Dec. 20, 2025), https://www.nysenate.gov/newsroom/press-releases/2025/liz-krueger/statement-senator-liz-krueger-and-assemblymember-linda [https://perma.cc/EU9F-ED3C].

218. New York Health Information Privacy Act, S.B. 929, 2025-2026 Leg., Reg. Sess., § 1122(1) (N.Y. 2025).

219. *Id.* § 1122(2)(b)(iv).

access and deletion mechanism, and canceling or deleting an online account would be treated as a request to delete the individual's health information.[220]

Like Washington, New York is building a web of shield and data privacy laws tailored to protecting reproductive health care. While these laws do not directly address data brokers, they certainly help prevent abortion information from falling into the hands of law enforcement. This legislative strategy—continually building out state abortion shield and data privacy laws in response to the dynamic circumstances of abortion prosecutions—is also prudent.[221] Since both abortion regulation and data-synthesizing technologies like GenAI are rapidly evolving, laws that "set it and forget it" will likely prove ineffective. States that truly care about protecting abortion data, providers, and patients should keep an eye on technological and regulatory developments and customize their targeted laws accordingly.

C. The Unmitigated Harm: Gaps in a Fragmented Legal Landscape

The preceding sections illustrate the patchwork of state and federal legislation that has sprung up to address abortion privacy and data brokers' inappropriate sale of personal information. Unfortunately, none of the existing laws directly address the phenomenon of private data brokers obtaining app data related to reproductive health and selling it to public entities. This section will summarize the gaps that remain under the existing law.

First, at the federal level, each of the four laws described above applies only to a narrow context. The FTC Health Breach Notification Rule only applies to health data, not other app data such as geolocation. Additionally, the "law enforcement exception" means that public notification of the data breach could often be postponed in the context of abortion investigations. The HIPAA Privacy Rule to Support Reproductive Health Care applies only to covered entities like health care providers and insurance companies—not tech companies and data brokers. The Fourth Amendment is Not for Sale Act is unenacted. Even if it became law, it only covers certain "stored communications"

220. *Id.* §§1122(3)(v), 1123(2)(b).

221. *See, e.g.*, Press Release, Protecting Reproductive Freedom: Governor Hochul Signs Legislation Affirming New York's Status as a Safe Haven for Reproductive Health Care (Feb. 3, 2025), https://www.governor.ny.gov/news/protecting-reproductive-freedom-governor-hochul-signs-legislation-affirming-new-yorks-status [https://perma.cc/GGM8-DBB7] (noting New York Governor Kathy Hochul's commitment to "taking action to strengthen protections for health care professionals and their patients" through expanding shield laws).

and would not encompass the full breadth of abortion app data that data brokers might sell to law enforcement. Lastly, the Protecting Americans' Data from Foreign Adversaries Act only regulates data disclosure to foreign powers and thus does not capture the provision of app data to domestic law enforcement. In sum, none of these federal laws remediates data brokers' sale of abortion app data to law enforcement.

The piecemeal state-by-state approach similarly fails to resolve data brokers' provision of abortion data. In general, most state laws seem to regulate *either* privacy for reproductive health care *or* data brokers but do not link these two issues. For instance, of the data broker regulation laws, only California and Nevada mention reproductive health data.[222] Similarly, state laws protecting reproductive health data, like New York's abortion shield or the Washington My Health My Data Act, do not reference data brokers.[223] To prevent data brokers from selling abortion information to law enforcement, these two problems should be considered and tackled together.

Another issue is that state comprehensive privacy laws like the CCPA only provide a privacy right to residents of the state that enacted the law. This means that California residents have a privacy right under the CCPA, but someone who travels to California to have an abortion from a state where it is illegal would not. As Figure 1 indicates, there is significant overlap between states that have no comprehensive privacy law, data broker regulation, or reproductive health privacy regime and states that have total or six-week abortion bans.[224] Additionally, of the states that have a total or six-week abortion ban and no relevant state legal regime, half of them have a poverty rate of fifteen percent or more, and all but three have a poverty rate of more than twelve percent.[225] In other words, it is in the poorest states in the country where abortion access is the most restricted *and* where there is the least privacy protection.

---

222. Nev. Rev. Stat. Ann. § 603A.430 (West 2025) (defining "consumer health data"); Cal. Civ. Code § 1798.99.82(b)(2)(c)–(e) (West 2025).

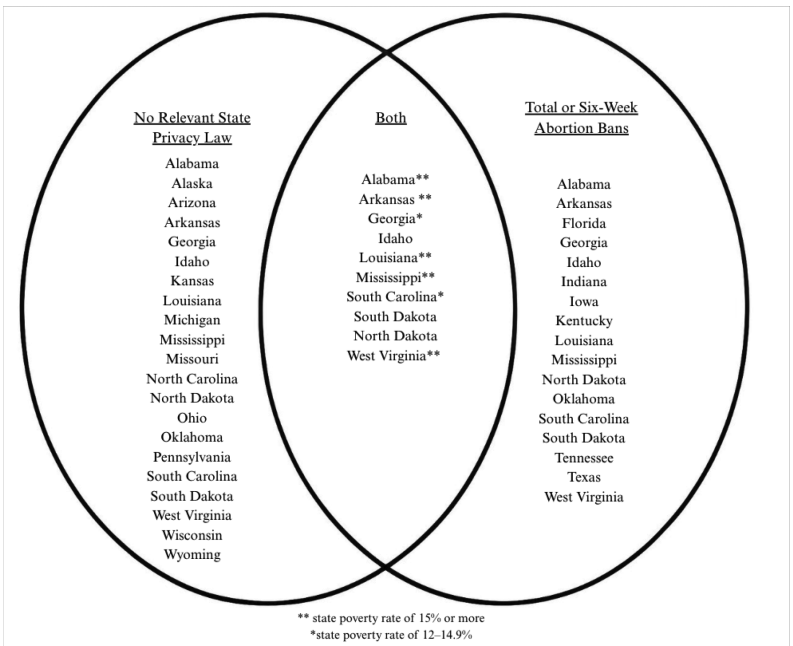
223. A keyword search for "data brokers" in both laws reveals that they do not include provisions referencing data brokers.

224. While this graphic was manually created, the list of states with "no relevant" state law was created using GenAI. First, the AI was prompted for lists of states that had (1) Comprehensive Privacy Laws, (2) Data Broker Regulations, or (3) Reproductive Health Privacy Laws/Abortion Shields. These lists were compared to the author's previous research for accuracy. The AI was then asked to provide a list of states that had no law in any of the three categories. The list of total or 6-week abortion bans is from KFF's abortion dashboard. *See Abortion in the United States Dashboard*, *supra* note 9.

225. *See* Craig Benson, U.S. Census Bureau, ACSBR–022, American Community Survey Briefs, Poverty in States and Metropolitan Areas: 2023 (2024).

This is especially concerning given that approximately half of all U.S. abortions are provided to Americans living below the poverty line.[226]

Figure 1: Overlap between states with abortion bans and states without data privacy laws



Although restricted access to abortion clinics could lead more women to turn to the internet for reproductive health advice, the digital trail created by web searches enables government surveillance of abortion.[227] This problematic dynamic is supported by empirical studies which suggest that the internet is a major source of information about pregnancy and abortion, particularly within vulnerable populations.[228]

226. Michelle Oberman, *What Will and Won't Happen When Abortion Is Banned*, 9 J.L. & Biosciences 1, 4 (2022).

227. Conti-Cook, *supra* note 15, at 5–6.

228. *See* Xun Wang & Robin A. Cohen, Nat'l Ctr. for Health Servs., Ctr. for Disease Control & Prevention, Health Information Technology Use Among Adults: United States, July–December 2022 (2023) (finding that 58.5% of adults used the internet to look for health or medical information, with a higher prevalence observed among women compared to men); Marzieh Javanmardi et al., *Internet Usage Among Pregnant Women for Seeking Health Information: A Review Article*, 23 Iranian J. Nursing & Midwifery Rsch. 79, 80 (2018) (finding that 81.50% of pregnant women across sixteen studies searched the internet for

In states with abortion bans, the internet might be the best source for obtaining accurate information about abortion. For instance, crisis pregnancy centers—which have a stated goal of preventing abortions—often provide clinically inaccurate information and deceptively delay access to comprehensive health care.[229]

The current law forces Americans—and especially vulnerable populations—to choose between using beneficial apps or internet searches to make reproductive health care choices and protecting their reproductive health data from law enforcement. This dynamic violates basic decisional autonomy. Americans should be able to choose to have an abortion *and* control who knows about it. Under existing law, they do not have this power.

III. Policy Suggestions

This section will explore policy changes to mitigate the violation of constitutional rights, basic privacy interests, and decisional autonomy embedded in the data broker loophole. Although the most straightforward way of addressing the data broker issue is to simply ban government entities from buying abortion app data from data brokers, other "backup" policy suggestions are also explored.

A. Ban Governments from Buying Personal Health Data from Data Brokers in the Reproductive Health Context

The first and most obvious solution to the data broker loophole in the abortion context would be simply prohibiting governments from purchasing abortion app data from data brokers. Given the borderless nature of data, such sales could certainly impact interstate commerce.[230] Thus, congressional authority to regulate data brokers' sale of abortion

---

health information during the first trimester); Adam Poliak et al., *Internet Searches for Abortion Medications Following the Leaked Supreme Court of the United States Draft Ruling*, 182 JAMA Internal Med. 1002, 1003 (2022) (finding that searches for abortion medications during the seventy-two-hour period after the *Dobbs* draft opinion leaked were cumulatively 162% higher than expected); Laura E. Dodge et al., *Quality of Information Available Online for Abortion Self-Referral*, 132 Obstetrics & Gynecology 1443 (2018) (noting that, of the 3.4 million Google searches for abortion clinics in the United States in 2015, individuals living in areas with restrictions on abortion access were the most likely to use the internet to search for these services).

229. Kate Coleman-Minahan et al., Youth Abortion Rsch. Project, Young People's Interactions with Anti-Abortion Centers: Deception, Inaccurate information, Delayed Care, and Violated Autonomy 1 (2025) (describing research suggesting that crisis pregnancy centers are "deceptive about their services, target people of low-income, provide clinically inaccurate information, attempt to change people's pregnancy decision and delay access to health care.").

230. U.S. Const. art. I, § 8, cl. 3.

app data could seemingly be derived from the Commerce Clause. Further support for Commerce Clause authority can be found in previous pro-abortion regulation. For instance, the Freedom of Access to Clinic Entrances Act of 1994 invoked the Commerce Clause to "protect and promote the public safety and health and activities affecting interstate commerce by establishing federal criminal penalties and civil remedies for certain violent, threatening, obstructive and destructive conduct that is intended to injure, intimidate or interfere with persons seeking to obtain or provide reproductive health services."[231] However, given the intense political and moral controversy around abortion, it might be difficult to pass a federal law explicitly protecting reproductive health data.

If federal legislation is not a possibility, states could enact laws preventing data brokers' sale of abortion information. Only five states have data broker regulation laws, and in most of these jurisdictions, the law is merely a registration or notice requirement rather than an affirmative prohibition.[232] These state laws should ideally prevent data brokers from sharing consumers' personal app data with third parties, such as law enforcement and provide individuals a deletion right. Laws that inform consumers that data brokers are collecting and using their personal information without giving consumers any mechanism to regain control over their own data do little to close the loophole.

If legislation banning data brokers' sale of abortion app data to law enforcement is not possible, the following policy proposals might help mitigate the issue.

B. Prohibit Companies and Data Brokers from Retaining Personal Data Indefinitely

It is reasonable that websites and apps collect personal data to deliver beneficial services, like menstrual cycle tracking, to consumers. That said, the tech companies that operate these platforms do not need to keep consumer data *indefinitely*. Such retention likely happens more often than consumers realize. For instance, a 2024 FTC report on a number of large tech companies called their data retention practices "woefully inadequate" and found that "some companies did not delete all user data in response to user deletion requests."[233] Timely deletion

231. Freedom of Access to Clinic Entrances Act of 1994, 18 U.S.C. § 248.

232. *See supra* Section II.B.2. Those five states are California, Nevada, Oregon, Texas, and Vermont.

233. *See* Press Release, Fed. Trade Comm'n, FTC Staff Report Finds Large Social Media and Video Streaming Companies Have Engaged in Vast Surveillance of Users with Lax Privacy Controls and Inadequate Safeguards for Kids and Teens (Sep. 19, 2024),

likely reduces the amount of data sold to data brokers or turned over to law enforcement, so reforming retention policies could be an effective way to combat inappropriate transmission of personal data to third parties.

A good proxy for the appropriate time to delete consumer data is simply whenever a consumer deletes their account. If the consumer no longer requires the service, then the data is seemingly only retained for monetization purposes. Using consumer account deactivation as a signal to delete data is reflected in recent legislative efforts, such as New York's S.B. 929, which provide that deleting an online account is treated as a request to delete the individual's health information.[234]

If a consumer affirmatively requests that their data be deleted, then certainly the company should be required to delete it then. Laws like the CCPA give individuals an explicit right to request deletion of their personal data, and companies (once this provision becomes effective) have an obligation to comply.[235] Such deletion laws also require a robust enforcement mechanism. California created a Privacy Protection Agency tasked with administering and enforcing the CCPA, but it remains to be seen whether this regulatory body will effectively ensure that companies actually delete consumer data upon request. Adequate enforcement likely requires an audit mechanism to ensure that companies are deleting information.[236] Without such oversight, it is difficult for consumers to ensure that their data was truly deleted by the company or data broker holding it.

Given concerns about deletion feasibility in the GenAI context,[237] legislators must be well-informed about actual technological capabilities and tailor laws accordingly. While deleting consumer information from a traditional database is straightforward, legislators and technology scholars must closely collaborate to come up with effective deletion solutions for information contained in GenAI models.

---

https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance [https://perma.cc/27B3-TUZ7].

234. S.B. 929, 2025-2026 Leg., Reg. Sess., §§ 1122(3)(v), 1123(2)(b) (N.Y. 2025).

235. Cal. Civ. Code § 1798.99.86(b) (West 2025).

236. Auditors would also need audit standards, so a standard-setter similar to the American Institute of Certified Public Accountants ("AICPA") or Public Company Accounting Oversight Board ("PCAOB") in financial audits would likely be required here.

237. *See* Feder Cooper, *supra* note 154, at 11–12 (explaining that, while compliance with data deletion laws like the CCPA might be feasible in the case of a traditional dataset, deletion in newer technological contexts—like AI—"may be less feasible or require 'disproportionate effort'").

C. Flip the Default Rule from Opt-Out to Opt-In and Strive for Meaningfully Informed Consent

Lawmakers should also carefully consider default rules in state legal regimes. Some of the laws discussed above give consumers an opt-out right, allowing them to ask companies to stop selling or sharing their data.[238] A more protective default rule, however, would be that companies cannot sell or share consumer data *until consumers opt in*. Given the sensitive nature of reproductive health data and other information that can be used to investigate people seeking abortions, an opt-in regime is preferable to an opt-out regime.

An opt-in default rule would not be without issues. As alluded to throughout this paper, an opt-in stands for little if consent is not meaningfully informed. The Washington My Health My Data Act uses an opt-in regime for personal health data and lays some basic ground rules to beef up consent.[239] For instance, "consent" under the MHMDA cannot be obtained through a general terms document that slips in a provision about sharing of consumer data.

At a minimum, consent to data sharing should be directly presented to consumers and free from quasi-deceptive inducements. It is inappropriate, for instance, to assume consent to data sharing from a sweepstakes entry.[240] Given that most consumers don't read the adhesion contracts they are bombarded with on the internet, informed opt-in should be as interactive and specific as possible. Appropriate consent is a delicate balancing act because the consumer needs to have sufficient information, but if the disclosure is too long, nobody will read it. Of course, any opt-in to data sharing could also be retracted if a consumer changes their mind about their data preferences. An opt-in default rule would not be perfect, but it would at least flip the default away from an assumption that data sharing and retention is acceptable unless a consumer takes it upon themselves to affirmatively opt out.

---

238. CAL. CIV. CODE § 1798.120 (West 2025) ("A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing.").

239. Under the MHMDA, "a regulated entity or a small business may not collect any consumer health data except . . . [w]ith consent from the consumer"—in other words, unless the consumer opts in. WASH. REV. CODE ANN. § 19.373.030(1)(a)(i) (West 2024).

240. *See, e.g.*, *Ovia Giveaway Rules*, *supra* note 22.

D. Abortion Shield Laws Should Mention Data Brokers Specifically

State abortion shield laws would be strengthened if they addressed data brokers specifically. For instance, the Washington shield law prohibits out-of-state governments from *subpoenaing* information about the provision or receipt of "protected health care services" in Washington, but it does not prevent a data broker from *selling* data to these same governments.[241] Since states like New York seem open to adapting their shield laws to changing circumstances, closing this loophole might not be too difficult. Given that abortion-seekers in states where abortion is illegal may seek the abortion pill online or research abortion clinic locations in other states, preventing data brokers from transmitting their digital trail to law enforcement is crucial to protecting abortion seekers, providers, and helpers from criminal sanctions.

E. Recognizing Evidentiary Privilege for Parent-Child Communications

A final policy change that might help rectify the data broker issue in the abortion context is a change in evidentiary privileges. Currently, parent-child communications are not privileged under the Federal Rules of Evidence, and only a handful of states recognize a parent-child privilege.[242] Given the apparent similarities between the parent-child relationship and the spousal relationship (which does garner evidentiary privilege at the federal level), scholars have argued that a narrow parent-child privilege, specific to the *Dobbs* context, could help protect minor children seeking abortions.[243]

Such a privilege could be powerful in a case involving pregnant minors communicating about abortion electronically with their parents. For instance, the Facebook messages between Celeste Burgess and her mother about obtaining abortion pills would have been inadmissible if a parent-child privilege existed in Nebraska. Given that thirty-six states require some combination of parental consent or notification when a minor child has an abortion, such digital communications about abortion

241. *See* WASH. REV. CODE ANN. § 7.115.020(2)(d)(i)(A) (West 2024) (prohibiting responses to subpoenas of reproductive health information). A keyword search of the law reveals that there is no mention of data brokers.

242. States that have recognized parent-child privilege as of 2024 include Connecticut, Idaho, Minnesota, Massachusetts, New York, and Washington. *See* Nila Bala, *Parent-Child Privilege as Resistance*, 65 B.C. L. REV. 2629, 2636 (2024).

243. *Id.* at 2661–67 (proposing a resistance-based parent-child privilege given that parental consent is needed for abortion in many states—without such a privilege, communications between the parent and child about the abortion can be admitted as evidence).

are likely common.[244] While a parent-child privilege would not solve the issue of data brokers selling communications to law enforcement, it could at least prevent the electronic communications that are sold from being admitted to court in the narrow case of a minor child who obtained an abortion.

Conclusion

The post-*Dobbs* landscape is messy: There is no longer a fundamental right to abortion in America, and though many states have tried to enact protections to safeguard the right to choose, criminal prosecution remains a real possibility for abortion seekers and providers. These issues are exacerbated by the general lack of data privacy in America, particularly the longstanding, nefarious connection between law enforcement and data brokers. The medley of federal and state legislation attempting to address these issues, while right-minded, does not fully remediate the circumvention of constitutional protections that takes place when law enforcement buys information from a data broker rather than obtaining the required subpoena, warrant, or court order. Neither does it prevent the criminalization of basic reproductive freedoms, even when they are obtained and provided in states where abortion is legal. To protect reproductive data privacy, a law prohibiting government entities from purchasing abortion app data from private parties is essential. Data profiteering is a big business, so making this change would be challenging. But to better safeguard constitutional rights, basic privacy interests, and reproductive freedom, such legislation is essential.

244. *Parental Consent/Notification Requirements for Minors Seeking Abortion*s, KFF (Sep. 2024), https://www.kff.org/womens-health-policy/state-indicator/parental-consentnotification/?currentTimeframe=0&sortModel=%7B%22colId%22:%22Location%22,%22sort%22:%22asc%22%7D [https://perma.cc/STP5-M3BN].