DIGITAL INTRUSION ON PHYSICAL PRIVACY: PROPOSING A STATE-BASED MODEL FOR HEALTH DATA PROTECTION POST-*DOBBS*

Emily G. Hinton*

ABSTRACT

Today, personal health information is at the mercy of a surveillance infrastructure built around the exploitation and sale of data on the private market. Existing health privacy laws, such as HIPAA, are woefully unequipped to address the risks and data practices of the digital era. Health data is collected, inferred, and sold online at alarming rates, leaving individuals vulnerable to privacy violations through the sharing of the most intimate information about their bodies. The overturning of *Roe v. Wade* and the criminalization of abortion in some states has created especially strong risks around reproductive health information; with individual health data so easily accessible, law enforcement and other interested third parties are able to circumvent procedural barriers and obtain deeply private health information without obstacle.

This Note argues that, in the absence of federal data privacy legislation, states must address the problem of reproductive health data surveillance through targeted state legislation. Washington's My Health My Data Act (MHMDA) is analyzed as an example of state data privacy legislation that closes gaps left by HIPAA and protects sensitive health data. Its strengths are identified through comparison to other data privacy legislation, both at home and abroad, to in turn recommend a model of health data privacy legislation for other states to adopt.

States must take advantage of the potential state law holds to safeguard rights and protections beyond current federal guarantees. Not only can greater reproductive health privacy be secured for

* Emily G. Hinton, J.D., Columbia Law School, 2026. A special thank you to the *HRLR* staff for their hard work and contributions to this Note.

residents of states that enact such legislation; widespread state adoption of health data privacy statutes can bring about a shift in norms for data collection and health information privacy practices nationwide.

TABLE OF CONTENTS

INTRODUCTION

Reproductive health surveillance has become a growing threat in the aftermath of the U.S. Supreme Court's decision to overturn *Roe v. Wade*.[1] This move not only represented an abandonment of the notion that decisions of this nature are protected by an inherent right to physical privacy; it also initiated a return to an era of abortion criminalization.[2] Allowing the prosecution of a medical act creates a new demand among law enforcement for medical—specifically, reproductive—information. This information, however, is not accompanied by privacy standards that meet the needs of the digital age. While the contents of one's home are constitutionally protected from police inspection,[3] the same cannot be said of reproductive health data. The collection and proliferation of such data—regardless of its deeply personal nature—has created a world where information about the state of one's body is less private than the physical contents of one's bedroom.

The collection, sale, and use of reproductive health data by various apps and websites is a central cause for concern. The Federal Trade Commission (FTC) recently sued Flo, a popular menstrual tracking app, for misleading users about its disclosure of their health data to third parties.[4] Despite promising privacy, Flo shared intimate reproductive health information with various marketing and analytics firms, all without the knowledge or consent of its millions of users.[5] As emerging stories like this demonstrate the potential for

---

1. *See generally* Roe v. Wade, 410 U.S. 113 (1973) (declaring Texas criminal abortion laws prohibiting abortions at any stage of pregnancy, except to save the life of the mother, unconstitutional in violation of the Due Process Clause of the Fourteenth Amendment).

2. *See* Dobbs v. Jackson Women's Health Org., 597 U.S. 215, 255–59 (2022) ("Our Nation's historical understanding of ordered liberty does not prevent the people's elected representatives from deciding how abortion should be regulated.").

3. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their . . . houses . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the . . . things to be seized.").

4. 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/X4W4-2SEJ].

5. *Id.*

data-based, digital monitoring of personal health, U.S. women are expressing significant concern over the privacy of their reproductive health data.[6] Still, the purchase of consumer health data from third parties remains unregulated at the federal level.[7] The worrying reality is that the collection and sale of private health information by apps like Flo is not prohibited by HIPAA or any other federal law.[8] The lack of reproductive health data privacy in the United States opens the door for exploitation of personal data, not only in a for-profit data market, but also in criminal prosecutions by states that have banned abortion.[9]

This Note will address the problem of reproductive health data surveillance by proposing a model for state-based data privacy protection through the adoption of targeted legislation. This model emphasizes the potential of state law to safeguard rights and protections beyond current federal guarantees. Given the urgent need for health data protection, state governments should not wait and hope for federal legislation to address the issue.[10] Widespread state adoption of health data privacy statutes can bring about a shift in norms for data collection and health information privacy practices. Even patchwork privacy protection across states can help ensure

---

6. *See* JIAXUN CAO ET AL., "I DELETED IT AFTER THE OVERTURN OF ROE V. WADE": UNDERSTANDING WOMEN'S PRIVACY CONCERNS TOWARD PERIOD-TRACKING APPS IN THE POST ROE V. WADE ERA 2 (2024) (summarizing survey results indicating that U.S. women are seriously concerned about the privacy practices of period tracking apps, but feel powerless to mitigate these privacy risks).

7. *See* Rhea Bhatia, *A Loophole in the Fourth Amendment: The Government's Unregulated Purchase of Intimate Health Data*, 98 WASH. L. REV. 67, 93 (2024) (explaining that there is no federal legislation that adequately addresses the collection and sale of personal data by third-party data brokers).

8. *See infra* Part I.B (detailing the current landscape of health privacy legislation).

9. *See infra* Part I.A. (discussing how data enters the private market and from there may be employed in criminal cases).

10. The federal government has not just been slow to enact data privacy reform; it has actively embedded domestic data surveillance in its operations. Sheera Frenkel & Aaron Krolik, *Trump Taps Palantir to Compile Data on Americans*, N.Y. TIMES (May 30, 2025), https://www.nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html (on file with the *Columbia Human Rights Law Review*); *see also* Jay Stanley, *Surveillance Businesses Have Human Rights Responsibilities*, ACLU (Sept. 22, 2025), https://www.aclu.org/news/privacy-technology/surveillance-human-rights [https://perma.cc/5RX8-9JP6] (calling for data surveillance companies to cease participation in the Trump Administration's immigration enforcement and related human rights abuses).

health data is better protected not just within individual state borders but across the nation.

Some states have already taken steps to establish health data privacy. This Note argues that Washington's My Health, My Data Act (MHMDA)[11] succeeds in protecting reproductive health data and other states should implement something similar. Part I describes the post-*Dobbs* legal and regulatory landscape, as well as the current state of reproductive health data privacy. Part II compares state laws enacted post-*Dobbs* to identify their relative strengths. It also compares these statutes to the European Union's data privacy law—the General Data Protection Regulation (GDPR)[12]—to examine the merits of a rights-based approach to data privacy. Part III proposes a model for state data privacy protection based on an analysis of gaps in existing legislation. States should adopt legislation with additional protections beyond what the MHMDA provides, such as a total ban on the sale of health data, front-end data minimization, and further procedural safeguards.

I. PRIVACY CONCERNS IN THE AFTERMATH OF *DOBBS*

The U.S. Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*[13] opened the door for state criminalization of abortion. When *Dobbs* was decided, thirteen states already had "trigger laws" on the books, which went into effect to ban abortion automatically once *Roe*'s protections were overturned.[14] Several of these states do not allow exceptions for incest or rape.[15] Since then, four additional states have banned abortion after six

11. WASH. REV. CODE § 19.373.005 (2023).

12. 2016 O.J. (L 119).

13. Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022).

14. *See* Jesus Jiménez & Nicholas Bogel-Burroughs, *What are abortion trigger laws and which states have them?*, N.Y. TIMES (June 24, 2022), https://www.nytimes.com/2022/06/25/us/trigger-laws-abortion-states-roe.html (on file with the *Columbia Human Rights Law Review*) (summarizing abortion trigger laws in thirteen states—Arkansas, Idaho, Kentucky, Louisiana, Mississippi, Missouri, North Dakota, Oklahoma, South Dakota, Tennessee, Texas, Utah, and Wyoming). One of these states, Missouri, has since voted to enshrine abortion protections in the state constitution. Allison McCann & Amy Schoenfeld Walker, *Tracking Abortion Laws Across the Country*, N.Y. TIMES, https://www.nytimes.com/interactive/2024/us/abortion-laws-roe-v-wade.html (on file with the *Columbia Human Rights Law Review*) (last updated May 15, 2026, at 12:02 ET) (tracking changes in state abortion legislation).

15. *See* Jiménez & Bogel-Burroughs, *supra* note 14 (detailing the abortion restrictions by state).

weeks, two states have banned abortion after twelve weeks, and Utah has banned abortion after eighteen weeks.[16]

Some states have also passed laws imposing civil liability on individuals who aid others in obtaining an abortion. For example, Texas's Heartbeat Act allows private parties to bring lawsuits against abortion providers and anyone who "aids and abets" an abortion.[17] These statutes create uncertainty as to what may be properly considered aiding and abetting an abortion, especially when taking the complexity of inter-state litigation and regulatory differences into account.[18] They also may incentivize private parties to seek out the intimate health information of others, whether through individual monitoring or more sweeping data purchases,[19] in order to bring private actions against them.[20] With both law enforcement and

16. *See* McCann & Walker, *supra* note 14 (detailing the state of abortion laws across the country).

17. Texas Heartbeat Act, TEX. HEALTH & SAFETY CODE ANN. §§ 171.201–171.212 (West 2021); *see also* Oklahoma Heartbeat Act, OKLA. STAT. tit. 63 §§ 1-745.31–1-745.44 (2022) (similarly allowing for lawsuits against providers as well as aiders and abettors).

18. *See* Sarah M. Hall et al., *The perils of navigating post-Dobbs anti-enforcement regimes*, LEGAL DIVE (Sept. 6, 2022), https://www.legaldive.com/news/Navigating-dobbs-state-antiabortion-enforcement-regimes-roevwade-epsteinbeckergreen-heartbeatlaw/631168 [https://perma.cc/5643-LED5] (discussing how companies should navigate the changing abortion legal landscape).

19. Commercial surveillance by data brokers makes sensitive data available for purchase by private parties. *See, e.g.*, Press Release, FTC, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other [https://perma.cc/T9VV-BTQJ] (detailing Kochava's sale of geolocation data used to tie individuals to reproductive health clinics).

20. They may also result in lawsuits against organizations that provide reproductive healthcare and information. Texas Right to Life threatened to sue abortion providers and healthcare workers at Planned Parenthood centers in Texas. Press Release, Planned Parenthood, BREAKING: IN WIN FOR ABORTION PROVIDERS, TEXAS STATE COURT GRANTS RESTRAINING ORDER AGAINST TEXAS RIGHT TO LIFE (Sept. 3, 2021), https://www.plannedparenthood.org/about-us/newsroom/press-releases/breaking-in-win-for-abortion-providers-texas-state-court-grants-restraining-order-against-texas-right-to-life (on file with the *Columbia Human Rights Law Review*). Planned Parenthood obtained a temporary restraining order against Texas Right to Life to bar these lawsuits while the Heartbeat Act's constitutionality is challenged. *Id.* Their standing to bring this suit was affirmed by the Texas Third Circuit Court of Appeals. Texas Right to Life v. Van Stean, No. 03-21-00650-CV, 2026 WL 118486, at *1 (Tex. App. Jan. 16, 2026).

private entities incentivized to obtain reproductive health information, it is essential that potential sources of health data leaks be identified and addressed.

A. The Role of Reproductive Health Data

Privacy experts have warned Americans that reproductive health data collected by various apps may be used to prosecute individuals seeking abortions.[21] A startlingly wide array of apps and websites collect intimate health data that may be used in a criminal prosecution,[22] and current privacy policies are often inadequate to protect this data from being shared. While consumers may expect some amount of health data sharing from apps which seek direct input of their health information, there are many more online entities harvesting this data from unsuspecting users through inferences and data analysis.

1. Data Collection

The most direct method of reproductive health data collection comes in the form of apps and other devices that track menstrual cycles, fertility, and pregnancy. Following the Supreme Court's decision to overturn *Roe v. Wade*, the White House warned Americans to be "really careful" using these apps due to concerns over the collection of reproductive health information.[23] Some apps obtain health data from a wearable, pregnancy-monitoring device.[24] Others

---

21. Rina Torchinsky, *How period tracking apps and data privacy fit into a post-Roe v. Wade climate*, NPR (June 24, 2022), https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps [https://perma.cc/R3KY-4CMZ].

22. *See, e.g.*, Binns et al., *Third Party Tracking in the Mobile Ecosystem*, *in* WEBSCI '18: 10TH ACM CONFERENCE ON WEB SCIENCE 23, 25 (2018) (finding that 90.4% of apps share data with at least one third-party tracker).

23. Jasmine Wright & Maegan Vazquez, *White House says Americans should be 'really careful' about using period tracker apps*, CNN (July 8, 2022, at 15:19 ET), https://www.cnn.com/2022/07/08/politics/white-house-period-tracker-apps/index.html (on file with the *Columbia Human Rights Law Review*).

24. *See* Laura Harrison, *How pregnancy monitoring technology contributes to the war on women*, WASH. POST (July 8, 2019), https://www.washingtonpost.com/outlook/2019/07/08/how-pregnancy-monitoring-technology-contributes-war-women (on file with the *Columbia Human Rights Law Review*) (discussing how the Owlet Band and other consumer wearable pregnancy monitors may contribute to reproductive surveillance).

ask the user to input their information directly, like popular period-tracking app Flo, which has millions of users.[25]

One U.K. poll found that a third of survey participants used a reproductive health app; the rate was higher for younger age groups, with 69% of 18 to 24 year-olds reporting they had used an app to track their periods.[26] But despite their widespread use, most of the reproductive health apps on the market today fail to meet basic data privacy standards. The Mozilla Foundation, a non-profit dedicated to building more ethical technology, found that eighteen out of twenty-five popular period apps and wearable devices posed major privacy risks.[27] Most of the apps they investigated did not provide clear guidelines on what data could be shared with law enforcement, or when it could be shared; several failed to meet even minimum security standards.[28] Researchers noted that these apps collect an abundance of intimate data while ignoring best privacy practices, which "is scary when even the baseline security is shaky in apps used by millions of women post-*Roe* [*v.*] *Wade*."[29]

But the collection of reproductive health information is not limited to health apps. Retailers have a strong incentive to identify pregnant customers, due to the myriad of products they can advertise to expecting parents.[30] Target, for example, analyzes demographic information and purchase history to generate a "pregnancy

---

25. FLO, https://flo.health [https://perma.cc/Z6G5-KZB5] (last visited Oct. 21, 2024) ("Over 420 million people around the world use the Flo app to track their periods, ovulation, pregnancy, and perimenopause.").

26. Martyn Landi, *Period and fertility tracking apps scrutinised over data security concerns*, THE INDEP. (Sept. 7, 2023, at 19:10 ET), https://www.the-independent.com/tech/information-commissioners-office-b2407119.html [https://perma.cc/U2US-B7KW]; Shanti Das, *'Young women can fall pregnant very easily': inside the wild west of smartphone fertility apps*, THE GUARDIAN (Jan. 19, 2025, at 17:00 ET), https://www.theguardian.com/technology/2025/jan/19/young-women-can-fall-pregnant-very-easily-inside-the-wild-west-of-smartphone-fertility-apps [https://perma.cc/ENV8-RS9S].

27. *In Post Roe v. Wade Era, Mozilla Labels 18 of 25 Popular Period and Pregnancy Tracking Tech With *Privacy Not Included Warning*, MOZILLA (Aug. 17, 2022), https://foundation.mozilla.org/en/blog/in-post-roe-v-wade-era-mozilla-labels-18-of-25-popular-period-and-pregnancy-tracking-tech-with-privacy-not-included-warning/ [https://perma.cc/34VJ-F7KV].

28. *Id.*

29. *Id.* (italics added).

30. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (on file with the *Columbia Human Rights Law Review*) (explaining how and why companies use data analytics to target pregnant consumers).

prediction" score for its users, which can even identify an expected due date window.[31] In 2012, a father confronted Target management for advertising baby products to his teenage daughter, only to find out that she was in fact pregnant.[32] This incident demonstrates that companies have used behavior analytics to draw inferences about individuals' reproductive health for over a decade, which is deeply concerning from a data privacy perspective.[33] The average consumer, relying on common sense, likely does not assume that their everyday purchasing behavior is providing companies with detailed personal health information. Nor can the average consumer be reasonably expected to assume an act as simple as online shopping reveals such intimate information about their body. What's more, a consumer would have to essentially avoid online shopping from a company like Target altogether if they wanted to avoid leaving this sort of digital trail.

These tactics have given rise to a private market for the purchase and sale of consumer data. Data brokers collect everything from location data to social media information, then turn around and sell that data to advertisers and other interested third parties.[34] Because data brokers collect data from a number of publicly available sources, such as web browsing activities and other everyday online interactions, this data is largely compiled without consumer knowledge.[35] The lack of a direct relationship or interaction between consumers and data brokers means there is no meaningful

---

31. *Id.*

32. *Id.*

33. The rise of predictive AI may further amplify the ability of these entities to monitor and profile individuals' reproductive health. For a discussion of the dangers of AI surveillance in this context, see Céline Castets-Renard & Caroline Lequesne, *Abortion in the Age of AI: A Need for Safeguarding Reproductive Rights in the United States and the European Union*, 69 MCGILL L. J. 533 (2024).

34. *See* Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014, at 13:59 ET), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you [https://perma.cc/R5CL-ZT3C] (describing the consumer data industry and the types of information data brokers collect for the purpose of selling to interested parties); *see also* JUSTIN SHERMAN, DUKE SANFORD CYBER POL'Y PROGRAM, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS 2 (2021) (summarizing data gathering mechanisms employed by major data brokers).

35. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 46 (2014).

opportunity for notice and consent.[36] This is significant when information can be used to draw inferences regarding consumers' physical health and traits once compiled,[37] which creates additional opportunities for data brokers to profit from its sale. For example, one health insurer buying consumer purchase data to draw inferences from health-related purchases and actions[38] may impact the ability of individuals to obtain even non-reproductive healthcare once that data is sold. Data brokers are not currently required to keep any of this data private unless they directly use it for protected purposes such as housing, employment, insurance, or credit.[39] As a result, personal data has been openly shared through this market without meaningful consumer knowledge.

The data collection infrastructure that arose from this private market has had impacts beyond the sphere of advertising and profit, affecting those seeking reproductive healthcare even before *Dobbs*. Intimate information collected by reproductive health apps has long been worryingly accessible to third parties.[40] Data sharing between companies has also already enabled targeted anti-abortion ad

---

36. Data brokers' so-called privacy policies are not useful consent mechanisms where consumers are not aware that they have obtained their data in the first place. CAREY SHENKMAN ET AL., CTR. FOR DEMOCRACY & TECH., LEGAL LOOPHOLES AND DATA FOR DOLLARS: HOW LAW ENFORCEMENT AND INTELLIGENCE AGENCIES ARE BUYING YOUR DATA FROM BROKERS 10 (2021).

37. *See, e.g.*, Duhigg, *supra* note 30 (describing how data analytics are used to draw inferences relating to pregnancy).

38. *See* Jen Wieczner, *How the Insurer Knows You Just Stocked Up on Ice Cream and Beer*, WALL ST. J. (Feb. 25, 2013, at 18:50 ET), https://www.wsj.com/articles/SB10001424127887323384604578326151014237898 (on file with the *Columbia Human Rights Law Review*) (describing how insurance companies track consumer purchasing habits, such as grocery and retail history, to predict health risks and adjust wellness programs).

39. *See* Press Release, Fed. Trade Comm'n, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data [https://perma.cc/Z4K2-A295] ("There are no current laws requiring data brokers to maintain the privacy of consumer data unless they use that data for credit, employment, insurance, housing, or other similar purposes.").

40. Before consumers had to worry about potential criminalization, data sharing by these apps raised concerns about employer discrimination towards pregnant individuals. *See* Drew Harwell, *Is your pregnancy app sharing your intimate data with your boss?*, WASH. POST (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think (on file with the *Columbia Human Rights Law Review*) (discussing how period and pregnancy tracking app Ovia was used as a monitoring tool by corporate employers).

campaigns, as revealed by a recent investigation.[41] Although Facebook claims to have filters in place to block sensitive personal data collection, investigators found that Facebook collects visitor information from 88% of the 294 crisis pregnancy center websites studied.[42] This data was then tied to anti-abortion marketing groups, which targeted these users for anti-abortion messaging.[43]

Experts warn that government agencies could just as easily obtain this sort of data from companies like Facebook in order to identify individuals seeking an abortion.[44] From July to December 2023 alone, Facebook received 73,390 government data requests and produced data for over 88% of these requests.[45] The majority of these requests were made through the U.S. legal process via warrants, subpoenas, and other court orders.[46] Facebook messages, obtained through warrants, have already been used to investigate and prosecute alleged illegal abortions.[47]

2. Use in Prosecution

In accordance with typical search and seizure procedure, law enforcement can obtain data or digital communications from any company with a valid judicial warrant.[48] Companies have no choice

---

41. *See* Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Information on Would-Be Patients*, THE MARKUP (June 15, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients [https://perma.cc/3MKR-N6KG] (detailing Facebook's involvement in one such anti-abortion ad campaign).

42. These "crisis pregnancy centers" are organizations aimed at deterring abortion and operate with "virtually no rules." *Id.*

43. *Id.*

44. *Id.*

45. *Government Requests for User Data: United States*, META, https://transparency.meta.com/reports/government-data-requests/country/US/?source=https%3A%2F%2Ftransparency.facebook.com%2Fgovernment-data-requests%2Fcountry%2FUS [https://perma.cc/2NML-K3ED] (last visited Mar. 2, 2026).

46. *Id.*

47. Martin Kaste, *Nebraska cops used Facebook messages to investigate an alleged illegal abortion*, NPR (Aug. 12, 2022, at 14:49 ET), https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion [https://perma.cc/BK7U-9N24].

48. *See* Naomi Nix & Elizabeth Dwoskin, *Search Warrants for Abortion Data Leave Tech Companies Few Options*, WASH. POST (Aug. 12, 2022), https://www.washingtonpost.com/technology/2022/08/12/nebraska-abortion-case-

but to hand over the requested data in these instances. However, federal agencies are also able to bypass the warrant requirement with an administrative subpoena.[49] These subpoenas do not require prior judicial approval, but must be enforced by federal courts so long as the information sought is relevant to an investigation the agency has authority to conduct.[50] Congressional reports have noted that these subpoenas lack the safeguards of a typical judicial search warrant, and their use is more likely to result in unjustified intrusions of privacy.[51] But there are currently over 300 federal statutes which grant various forms of administrative subpoena authority to dozens of administrative agencies, allowing the government to compel companies to disclose sensitive personal data in their possession without typical constitutional protections.[52]

The current private data market enables law enforcement to further circumvent these legal processes. Experts have noted a concerning trend of government agencies obtaining data through commercial purchases from data brokers, often for pre-investigative inquiries or other intelligence operations where there is not yet a legal basis for a warrant or even a subpoena.[53] Agency procurement contracts typically refer to this data as "open source" or "publicly available," despite the fact that this data is often not knowingly made

---

facebook (on file with the *Columbia Human Rights Law Review*) (discussing Facebook's compliance with a search warrant in a Nebraska abortion investigation).

49. *See* CHARLES DOYLE, ADMINISTRATIVE SUBPOENAS IN CRIMINAL INVESTIGATIONS 8 (2012) (summarizing the administrative subpoena power with particular focus on criminal administrative subpoenas).

50. An administrative subpoena must be enforced unless it is "plainly incompetent or irrelevant to any lawful purpose of the [requesting official] in the discharge." Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943). Administrative subpoenas are subject to judicial review, but are only held to a reasonableness standard, not the probable cause standard applied to ordinary search warrants. United States v. Powell, 379 U.S. 48, 57–58 (1964) (articulating a four-part deferential standard of reasonableness review); *see also* Sec. & Exch. Comm'n v. Jerry T. O'Brien, Inc., 467 U.S. 735, 741–42 (1984) (explaining that the *Powell* analysis applies to all administrative subpoena authorities).

51. *See* DOYLE, *supra* note 49.

52. U.S. DEP'T OF JUST., REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES, https://www.justice.gov/archive/olp/rpt_to_congress.htm#2a [https://perma.cc/7SC3-YU5E] (last visited Mar. 2, 2026) (see Appendix A1 for a full list of statutes which grant administrative subpoena authority).

53. *See* SHENKMAN ET AL., *supra* note 36, at 22 (discussing findings on law enforcement use of data sourced from brokers based on a review of publicly available documents).

available to the public, nor made available for purchase by the consumer.[54] This open source designation allows law enforcement to evade Fourth Amendment privacy protections, leaving them free to purchase this information, no matter how revealing it is in nature.[55]

The accessibility of this data has raised concerns about its potential to fill gaps in cases brought against individuals for their pregnancy outcomes. In her article about digital reproductive surveillance, civil rights attorney and researcher Cynthia Conti-Cook noted that "when medical theories fail to explain why some outcomes happened, prosecutors can now sift through an accused person's most personal thoughts, feelings, movements, and medically-related purchases during their pregnancy, even if there is little evidence supporting the conclusion that their conduct caused the pregnancy to end."[56] The use of digital evidence to prosecute people for pregnancy outcomes predates *Dobbs*. In 2017, Latice Fisher was charged with second degree murder for having a stillbirth at home; the police attempted to use her internet search history, which included searches for abortion medication, as evidence of intent.[57]

Post-*Dobbs*, differences in abortion laws across states will likely lead to attempts at inter-state prosecutions.[58] Early last year, Dr. Margaret Carpenter of New York was indicted by a grand jury in Louisiana for allegedly prescribing abortion pills online to a girl in

---

54. *Id.* at 19–21.

55. *See infra* Part I.B (explaining the third-party doctrine exception to the Fourth Amendment).

56. Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV. 1, 50–51 (2020).

57. *See* Jia Tolentino, *We're Not Going Back to the Time Before Roe. We're Going Somewhere Worse*, NEW YORKER (June 24, 2022), https://www.newyorker.com/magazine/2022/07/04/we-are-not-going-back-to-the-time-before-roe-we-are-going-somewhere-worse [https://perma.cc/YMW7-QXR3] (detailing the case against Latice Fisher and the digital evidence seized by police). For additional examples of pregnancy-related prosecutions pre-*Dobbs*, see Runa Sandvik, *How US police use digital data to prosecute abortions*, TECH CRUNCH (Jan. 27, 2023, at 12:11 PT), https://techcrunch.com/2023/01/27/digital-data-roe-wade-reproductive-privacy [https://perma.cc/G7SX-A94L].

58. *See* ASSOCIATED PRESS, *Idaho governor signs ban on 'abortion trafficking'*, PBS NEWS (Apr. 6, 2023, at 10:01 AM ET), https://www.pbs.org/newshour/politics/idaho-governor-signs-ban-on-abortion-trafficking [https://perma.cc/NL8X-SWT4] (making it illegal to help minors leave the state for an abortion without parental consent). For an exploration of the complications that will arise from interjurisdictional legal conflicts over abortion, see David Cohen et al., *The New Abortion Battleground*, 123 COLUM. L. REV. 1 (2025).

Louisiana.[59] These sorts of prosecutions can be expected to increase,[60] and as they do, law enforcement's ability to track reproductive health information online will only grow more sophisticated. Currently, there are virtually no limits on their ability to obtain this intimate data; this lack of regulation is detailed below in Part I.B.

B. The Regulatory Landscape

Current prohibitions on the sharing of health information are limited to the healthcare sector. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) authorizes the Secretary of the U.S. Department of Health and Human Services (HHS) to issue national privacy regulations.[61] Under the HHS Privacy Rule, covered entities may not disclose individually identifiable health information, barring a few narrow exceptions.[62] In 2024, they issued the HIPAA Privacy Rule to Support Reproductive Health Care Privacy, which specifically prohibits covered entities from disclosing protected health information to those attempting to investigate or impose liability on individuals seeking or providing lawful reproductive healthcare.[63] However, in 2025, a Texas court issued an order vacating most provisions of this rule, eliminating the heightened reproductive

---

59. Anthony Izaguirre, *New York shields abortion pill prescribers after a doctor was indicted in Louisiana*, AP NEWS (Feb. 3, 2025, at 14:55 ET), https://apnews.com/article/abortion-pills-new-york-hochul-12dc697d30967808aed9c3e4db2b1ff2 [https://perma.cc/L9FY-YU8S].

60. All pregnancy-related prosecutions have increased following *Dobbs*; 2022–2023 saw the highest number of pregnancy-related prosecutions documented in a single year. WENDY A. BACH & MADALYN K. WASILCZUK, PREGNANCY AS A CRIME: A PRELIMINARY REPORT ON THE FIRST YEAR AFTER *DOBBS* 2 (2024).

61. Health Insurance Portability and Accountability Act of 1996, 29 U.S.C. §§ 1181–1183, 1191, 300gg, 1320a, 18 U.S.C. §§ 24, 1347, 669, 1035, 1518, 3486, 42 U.S.C. 1320d, 26 U.S.C. 220, 4980E, 7702B, 6050Q, 4980C, 9801_9806, 4980D, 6039F.

62. U.S. DEP'T OF HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 4–9 (2025), https://www.hhs.gov/sites/default/files/privacy summary.pdf (on file with the *Columbia Human Rights Law Review*).

63. Press Release, U.S. Dep't Health & Hum. Servs., The Biden-Harris Administration Issues New Rule to Support Reproductive Health Care Privacy Under HIPAA (Apr. 22, 2024), https://www.hhs.gov/about/news/2024/04/22/biden-harris-administration-issues-new-rule-support-reproductive-health-care-privacy-under-hipaa.html (on file with the *Columbia Human Rights Law Review*).

health data protections it sought to establish.[64] Further, health data collected by any non-covered entity does not fall under HIPAA protections.[65] Worryingly, companies outside the healthcare sphere are therefore not at all limited in their ability to disclose such data.

To be considered a business associate for purposes of the statute, the associate must be working directly on behalf of a covered entity to receive, maintain, or transmit protected health information.[66] Apps and websites, specifically, need only comply with HIPAA regulations if they were created for or directly contract with a covered healthcare organization.[67] This is a very narrow window, and excludes most health apps, which tend to be developed and operated independently of any specific health provider.[68] Retail companies like Target that collect or infer health data through their websites are similarly not HIPAA-regulated under this definition.[69] While many health tracking apps (such as Flo) purport to provide a healthcare-

64. Purl v. United States Department of Health and Human Services, No. 2:24-CV-228-Z, at 1 (N.D. Tex. June 18, 2025) (leaving intact only a few amendments related to providing notice of updated privacy practices).

65. Courts have generally interpreted the definition of "covered entities" very narrowly and have even determined that certain health providers do not fall within its scope. *See, e.g.*, United States v. Gray, 59 F.4th 329, 333–34 (8th Cir. 2023) (finding no basis to reject the Bureau of Prisons' own determination that it is not a "covered entity" under HIPAA).

66. 45 C.F.R. § 160.103.

67. *See* Steve Alder, *Majority of Americans Mistakenly Believe Health App Data is Covered by HIPAA*, THE HIPAA J. (July 26, 2023), https://www.hipaajournal.com/americans-mistakenly-believe-health-app-hipaa (on file with the *Columbia Human Rights Law Review*) ("HIPAA applies to HIPAA-covered entities . . . and vendors used by those entities, which are classed as business associates. While health apps may collect some of the exact same health data that is maintained by HIPAA-covered entities, [that information] is not subject to the same privacy and security standards."). Most Americans are unaware of this; in a survey, 81% of respondents believed that the health data collected by health apps is covered by HIPAA. *Id.*

68. *See Resources for Mobile Health App Developers*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html [https://perma.cc/6TGQ-4VE2] (Dec. 22, 2022) (listing tools for identifying whether an app is HIPAA-regulated, including a Health App Use Scenarios guide); U.S. DEP'T OF HEALTH & HUM. SERVS., HEALTH APP USE SCENARIOS & HIPAA (2016) [hereinafter HEALTH APP USE SCENARIOS], https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf (on file with the *Columbia Human Rights Law Review*) (outlining the narrow subset of apps developed as business associates of a covered entity).

69. *See* 45 C.F.R. § 160.103 (business associate definition).

adjacent service to consumers, these apps are commercial in nature and are generally not affiliated with any entities covered by HIPAA.[70]

The FTC may be more equipped to directly regulate data disclosure by commercial entities. President Biden acknowledged this in an executive order issued in 2022, which encouraged the FTC to "consider actions . . . to protect consumers' privacy when seeking information about and provision of reproductive healthcare services."[71] Still, the FTC's protection of reproductive health data is limited. Its Health Breach Notification Rule is its primary form of protection for health data not already covered by HIPAA.[72] However, this rule only creates obligations in the event of a breach of individually identifiable health information.[73] It does not prevent voluntary disclosure by these apps and companies.

The FTC's other main avenue for enforcement of data privacy is Section 5 of the FTC Act, which seeks to prevent deceptive practices generally.[74] Recently, period-tracking app Flo came under fire from the FTC for sharing users' health data without their knowledge or consent.[75] They reached a settlement over Flo's violation of Section 5 of the FTC Act, which prohibits companies from misleading consumers about their practices.[76] However, this provision only protects consumers from being actively misled by these companies. No regulation exists to prevent companies from sharing this information, so long as they are honest about it in their privacy policies.[77] Additionally, absent a consumer protection statute proscribing a specific practice, Section 5 enforcement under the FTC largely involves case by case determinations that a practice is

---

70. *See* HEALTH APP USE SCENARIOS, *supra* note 68 (explaining that such health apps fall outside HIPAA protections).

71. Protecting Access to Reproductive Healthcare Services, Exec. Order No. 14076, 87 Fed. Reg. 42053, 42054 (July 8, 2022).

72. Health Breach Notification Rule, 16 C.F.R. § 318 (2025).

73. *Complying with FTC's Health Breach Notification Rule*, FED. TRADE COMM'N (Jan. 2025), https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0 [https://perma.cc/VV6H-EFVJ].

74. 15 U.S.C. § 45(a)(1).

75. *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, FED. TRADE COMM'N (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google [https://perma.cc/UYE3-D88C].

76. *Id*;. Flo Health, Inc., No. C-4747, 2021 WL 2709281, at *1 (June 17, 2021).

77. *See* FTC Act, 15 U.S.C. § 45(a)(1) (prohibiting only "unfair or deceptive acts in or affecting commerce").

unfairly deceptive.[78] This fails to provide proscriptive certainty, and is subject to changes in internal policy, which is itself subject to changes in the executive administration. It is no substitute for legislation enshrining specific protections.

There is also no recognized Constitutional protection for this data. In *Smith v. Maryland*, the Supreme Court established the third party doctrine, holding that the Fourth Amendment does not protect information given voluntarily to third parties.[79] While the Court did establish an exception to this doctrine in *Carpenter v. United States*, it is exceptionally narrow.[80] There, the Court found that cell phone location data could not be obtained without a warrant because of the deeply revealing nature of the data, as well as the inescapable nature of its collection.[81] While some have argued that health data collected by apps and other digital platforms fall under the *Carpenter* framework,[82] the Supreme Court has not extended the exception to other types of data.[83]

While there could be a path forward for regulatory or constitutional protection of intimate health data, this Note will focus on the potential of legislation to address these issues. Enshrining data privacy in law can create lasting protection that is more insulated from the whims of the current executive administration and political landscape.

---

78. *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (July 2025), https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/UX97-KNMF]. The FTC defines a deceptive practice as something that involves a representation, omission, or practice that is likely to mislead the consumer. *Id.*

79. Smith v. Maryland, 442 U.S. 735, 743–45 (1979).

80. *See* Carpenter v. United States, 585 U.S. 296, 320 (2018) (establishing an exception for cell phone location information only).

81. *Id.*

82. *See* Sophie Nelson, *The Post-Dobbs Reality: Privacy Expectations for Period-Tracking Apps in Criminal Abortion Prosecutions*, 51 PEPP. L. REV. 783, 819 (2024) (arguing that the holding in Carpenter should be extended to personal information in period tracking apps).

83. The Supreme Court has not directly addressed the *Carpenter* exception again. Lower courts have generally declined to extend the exception to any data not closely analogous to cell-site location information. *See, e.g.*, United States v. Contreras, No. 17-11271, slip op. at 5 (5th Cir. Oct. 1, 2018) (declining to extend the *Carpenter* exception to IP address records because they did not reveal the defendant's "day-to-day movement").

II. COMPARING EXISTING PROTECTIONS

Many have called for federal data privacy legislation to correct the current lack of protection for personal data and information.[84] To this end, a bill called the American Data Privacy and Protection Act (ADPPA) was introduced in 2022, with the goals of "provid[ing] consumers with fundamental privacy rights, creat[ing] strong oversight mechanisms, and establish[ing] meaningful enforcement."[85] This bill, unfortunately, was never enacted, and it appears unlikely that any federal data privacy legislation will be enacted in the near future.[86] It is therefore up to states to establish these protections. This Part will identify and compare different forms of existing data privacy legislation, laying the groundwork for analysis of a strong state-based framework for health data protection.

A. State Legislation

A number of states have passed data privacy laws aimed at protecting health data. Currently, twenty states have enacted some form of broad consumer data privacy legislation,[87] while six states have passed narrower, more targeted data privacy laws.[88] The remaining twenty-four states—nearly half the country—lack any

84. *See, e.g.*, Sam Begland, *Stars, Stripes, and Surveillance: The United States' Failure to Regulate Data Privacy*, 38 AM. U. L. REV. 747, 781–83 (2023) (arguing that Congress must enact data privacy legislation to fulfill their obligations under the International Covenant on Civil and Political Rights); 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, 253 (2023) (arguing for the adoption of federal data privacy legislation to safeguard reproductive health data); Heather Chong, *Data for Sale: Navigating the Role of Data Brokers and Reproductive Health Information in a Post-Dobbs World*, 26 SMU SCI. & TECH. L. REV. 99, 110 (2023) (arguing for Congress to adopt ADPPA).

85. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

86. *See infra* notes 161–63 and accompanying text (discussing failures to implement federal legislation).

87. These states include California, Oregon, Montana, Utah, Colorado, Nebraska, Minnesota, Iowa, Texas, Indiana, Kentucky, Tennessee, Florida, Virginia, Maryland, Delaware, New Jersey, Connecticut, Rhode Island, and New Hampshire. *Which States Have Consumer Data Privacy Laws?*, BLOOMBERG LAW (Apr. 7, 2025), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#states-with-comprehensive-data-privacy-laws [https://perma.cc/5N9L-QJHW].

88. These states include Washington, Nevada, Michigan, New York, Vermont, and Maine. *Id.*

data privacy protections whatsoever.[89] California was one of the first states to establish a comprehensive data privacy law, but its broad provisions may be less effective at targeting health data for protection than narrower legislation passed after *Dobbs*.[90] Washington's more recent data privacy law accomplishes more in this regard by enacting targeted protection of intimate health data, although it doesn't establish broader consumer data rights.[91] These two states, as the strongest examples of each approach, will be compared in greater detail. Specifically, this Part will discuss the breadth of protection offered by each, their definition of terms, and any exceptions.

1. Washington

Washington's My Health, My Data Act (MHMDA),[92] enacted following the overturn of *Roe v. Wade*, is a landmark piece of legislation in the realm of health data privacy. The specific aim of the Act is to safeguard health data that does not fall under HIPAA's narrow protections.[93] The MHMDA is the first law to enact specific protections for personal health information not covered by HIPAA,[94] and is tailored to achieve that purpose.

The MHMDA defines "consumer health data" broadly as any personal information that "identifies the consumer's past, present, or future physical or mental health status."[95] Direct information about a consumer's condition, in addition to anything which indicates a consumer is seeking healthcare services (such as search history), falls under this definition.[96] Reproductive health and gender-affirming care information are both specifically identified as protected forms of physical or mental health status.[97] The MHMDA also takes its protections a step further; any information about a person's physical

89. *Id.*

90. *See infra* Part II.A.2 (detailing the lack of specific health data protection in the California Consumer Privacy Act).

91. *See infra* Part II.A.1 (detailing specific protections for health data in Washington's My Health, My Data Act).

92. WASH. REV. CODE § 19.373 (2023).

93. *Id.* § 19.373.005.

94. *Protecting Washingtonians' Personal Health Data and Privacy*, WASH. STATE OFF. OF THE ATT'Y GEN., https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy [https://perma.cc/E4U8-JTTX] (last visited Mar. 2, 2026) [hereinafter Washington AG FAQ].

95. WASH. REV. CODE § 19.373.010(8)(a) (2023).

96. *Id.* § 19.373.010(8)(b).

97. *Id.*

or mental health inferred from non-health information is also considered to be consumer health data.[98] This means knowledge of an individual's status derived from data analysis, such as Target's "pregnancy prediction score,"[99] is likely protected under the Act.

The MHMDA prohibits the collection of consumer health data except where it is necessary to provide the product or service, or where the consumer has given informed consent.[100] Necessity or consent is separately required in order to share that health data with a third party.[101] The sale of health data, however, is only permitted with the consumer's consent; the regulated entity must obtain separate signed authorization from the consumer, whose consent may be revoked at any time.[102] This authorization must disclose certain information to the consumer, most notably:

- the specific health data that will be sold;
- the identity of the purchasing entity (including their contact information);
- the purpose of the sale;
- a disclaimer that once sold, the data may be subject to redisclosure and may no longer be protected by the Act.[103]

From the start, an entity must disclose in its privacy policy the purpose of their data collection and how the data will be used, along with a list of any third parties they plan to share consumer health data with.[104] Consumers are granted the right to access their health data, withdraw their consent for collection or sharing, and delete the data at any time.[105] To aid in enforcement, the MHMDA

---

98. *Id.*

99. *See* Duhigg, *supra* note 30 (describing how retailers like Target identify pregnant customers); *see also* Washington AG FAQ, *supra* note 94 (answering frequently asked questions about the MHMDA).

100. WASH. REV. CODE § 19.373.030 (2023). To obtain informed consent, the entity must disclose the types of health data collected or shared, the purpose of collection or sharing, and what type of entity the data will be shared with. This disclosure must also include instructions for withdrawing consent in the future. *Id.* § 19.373.030(1)(c).

101. *Id.* § 19.373.030(1)(b).

102. *Id.* § 19.373.070.

103. *Id.*

104. *Id.* § 19.373.020.

105. *Id.* § 19.373.040. *See also* Amy Olivero & Anokhy Desai, *Washington's My Health, My Data Act*, IAPP (Apr. 25, 2023), https://iapp.org/resources/article/washington-my-health-my-data-act-overview

provides for a private right of action against entities that fail to comply with these regulations.[106]

There are three main elements that make the MHMDA unique compared to other legislation that will be discussed in this Note.[107] First, it explicitly includes reproductive, sexual, and gender-related health information as forms of protected health data.[108] Second, it protects location information that could indicate an individual's attempt to obtain healthcare.[109] Third, while it does include an exception to its ban on health data sharing for compliance with the law, this exception is limited to compliance with Washington state and federal law.[110] This means there is no obligation under the law to share this data with other states that may attempt to compel the sharing of reproductive health information. All three of these elements help protect consumers from potential criminal investigation and prosecution by other states with abortion bans in place.

2. California

California, by contrast, has a broader data privacy law on the books. The California Consumer Privacy Act (CCPA) of 2018 was passed with the aim of giving consumers more control over their personal data generally.[111] The CCPA puts in place several

---

[https://perma.cc/VA47-62UR] (explaining consumer rights and regulated entity obligations under MHMDA).

106. *See infra* Part III.A. (discussing the private right of action and its potential effects).

107. *See* Jacqueline Klosek, *Takeaways from Washington's Sweeping Health Privacy Bill*, GOODWIN (May 10, 2023), https://www.goodwinlaw.com/en/insights/blogs/2023/05/takeaways-from-washingtons-sweeping-health-privacy-bill [https://perma.cc/H6HV-SRL9] (noting three ways in which the MHMDA is unique from other legislation that allow the Act to have more impact).

108. *Id.*

109. *Id.*; WASH. REV. CODE § 19.373.010(8)(b)(xii) (2023).

110. Klosek, *supra* note 107. WASH. REV. CODE § 19.373.100(3) (2023). It is worth noting that in the event of a federal abortion ban, this provision would not prevent the sharing of health data with federal law enforcement. *See infra* note 233 and accompanying text (discussing the possibility of a federal ban).

111. Assemb. B. 375, 2018 Gen. Assemb., Reg. Sess. (Cal. 2018). The bill was passed unanimously but was propelled by a ballot initiative seeking increased data privacy rights in the state. It was opposed by various tech companies, including Google and Microsoft, who stand to gain from the sale of consumer data. Jon Brodkin, *California approves privacy rules opposed by ISPs and tech companies*, ARS TECHNICA (June 28, 2018), https://arstechnica.com/tech-

protections for Personal Information ("PI"), which it defines as any information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[112] The CCPA gives California citizens the right to know what PI is being collected, the right to delete PI held by businesses, the right to correct data inaccuracies, and the right to opt out of sharing PI, as well as the right to non-discrimination in the event they exercise these rights.[113] The CCPA also includes regulations that enforce data minimization by companies, meaning data should only be obtained insofar as it is reasonably necessary and proportionate to achieving a specific aim.[114] The CCPA was initially lauded as the "strongest privacy legislation" in the United States, [115] though this was prior to Washington's enactment of the MHMDA.

The CCPA is a comprehensive data privacy statute, but its protection of health data is less robust. While the CCPA is far-reaching in its application, it does not contain any heightened protections for health data, and was originally not tailored to address any of the concerns discussed in Part I.[116] Although biometric information is listed as a form of PI,[117] the term "biometric information" is itself defined as "an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity."[118] This definition centers the way biological information can be used to identify an individual, rather than acknowledging health information as a form of data worth

---

policy/2018/06/california-approves-privacy-rules-opposed-by-isps-and-tech-companies (on file with the *Columbia Human Rights Law Review*).

112. CAL. CIV. CODE § 1798.140(v)(1).

113. *Id.* §§ 1798.105–25; *see also* Jill Cowan & Natasha Singer, *How California's New Privacy Law Affects You*, N.Y. TIMES (Jan. 3, 2020), https://www.nytimes.com/2020/01/03/us/ccpa-california-privacy-law.html (on file with the *Columbia Human Rights Law Review*) (summarizing consumers' rights under the CCPA).

114. *See* CAL. CIV. CODE § 1798.100(a)(1), (a)(2), (c) (requiring that companies not collect data beyond what is necessary for the purposes they disclosed).

115. Conti-Cook, *supra* note 56, at 71.

116. *See supra* Part I.A (discussing the exploitation of personal data in a private market and its potential for use by law enforcement in criminal prosecutions).

117. CAL. CIV. CODE § 1798.140(v)(1)(E).

118. CAL. CIV. CODE § 1798.140(c).

protecting outside the identification context. The CCPA also clarifies that "publicly available" information is not covered by PI protections.[119] Although the statute excludes biometric data collected without an individual's knowledge from what may be considered "publicly available,"[120] it is silent on whether health information voluntarily given to an app or website is "publicly available" and free to be shared.

The CCPA also contains a few notable exceptions. If a business's obligations to the consumer restrict its ability to (1) comply with federal or state law, (2) comply with a court order or subpoena, (3) cooperate with law enforcement, or (4) cooperate with an agency seeking "emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury," it is exempt from such CCPA obligations.[121] These exceptions left reproductive health information vulnerable to law enforcement, and language referring to a risk of danger to "a natural person" raised questions in the context of abortion.[122] States that consider a fetus a natural person and seek to prevent an individual from obtaining abortion-related healthcare in a state where it is legal could draw on such language to demand health information from providers, apps, and more.

However, the California legislature has taken action to strengthen protections for reproductive health information in the aftermath of *Dobbs*. In 2023, the California legislature amended the CCPA to create a carveout for information related to reproductive healthcare services.[123] If a business has collected data "related to accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including, but not limited to, abortion services," the aforementioned exemption does not apply.[124] This means that data related to reproductive health services is not exempt from the CCPA's privacy protections when sought by law enforcement. Thus, while the CCPA does not ensure health data privacy broadly, it does help protect reproductive data from direct use in criminal prosecution.

---

119. CAL. CIV. CODE § 1798.40(v)(2)(A).
120. *Id.* § 1798.140(v)(2)(B)(ii).
121. *Id.* § 1798.145(a)(1).
122. *Id.* § 1798.145(a)(2)(A).
123. Assemb. B. 1194, 2023 Gen. Assemb., Reg. Sess. (Cal. 2023).
124. CAL. CIV. CODE § 1798.145(a)(2)(A).

The CCPA also regulates fewer entities than the MHMDA. Like the MHMDA, the CCPA may apply to any company that does business with California residents, even if it does not have a physical presence in the state.[125] But unlike the MHMDA, the CCPA sets a minimum threshold for which businesses are regulated. A business must be for-profit, and either (1) have a gross annual revenue over $25 million, (2) deal with the data of over 100,000 California residents or households, or (3) derive over half their revenue from selling the PI of Californians.[126] Nonprofits and small businesses are therefore not regulated under the CCPA. While this spares small businesses from the costs associated with compliance, it means not all health data is protected under the CCPA, and some Californians' data may still be collected and sold without their knowledge. The MHMDA does not have a similar minimum threshold for businesses and applies to nonprofit organizations as well.[127]

Overall, while the CCPA does provide some important protections, the MHMDA is more successful in protecting individual health privacy due to its broader definitions of health data, stronger consent and data collection restrictions, and robust enforcement mechanisms. It therefore stands as a more comprehensive example of health data privacy legislation for other states looking to implement similar protections. As such, the MHMDA will serve as the primary point of comparison for the GDPR for purposes of this Part.

---

125. *What Businesses Outside California Should Know About the California Consumer Privacy Act*, TANNENBAUM HELPERN (Mar. 20, 2019), https://www.thsh.com/publications/what-businesses-outside-california-should-know-about-the-california-consumer-privacy-act [https://perma.cc/9QH5-H3PD].

126. CAL. CIV. CODE § 1798.140(d). *See also California Consumer Privacy Act (CCPA)*, OFF. OF THE ATT'Y GEN. (Mar. 13, 2024), https://oag.ca.gov/privacy/ccpa [https://perma.cc/W9T6-FGLW] (answering frequently asked questions about the CCPA).

127. *See* Jami Vibbert, Nancy L. Perkins & George Eichelberger, *Beyond HIPAA and the State Consumer Privacy Laws: Washington State's New "My Health, My Data Act,"* ARNOLD & PORTER (May 12, 2023), https://www.arnoldporter.com/en/perspectives/advisories/2023/05/beyond-hipaa-and-the-state-consumer-privacy-laws [https://perma.cc/468G-KMUL] (discussing the MHMDA's broad jurisdictional scope). The statute did, however, give small businesses more time to come into compliance with the requirements of the MHMDA. *See, e.g.*, WASH. REV. CODE § 19.373.030(2) (2023) (granting small businesses additional time to comply with consumer consent provisions).

B. The E.U. Approach

Having identified the strengths and pitfalls of current state data privacy legislation, it is useful to compare it to one of the highest standards for data privacy legislation outside of the United States: the European Union's General Data Protection Regulation (GDPR).[128] Although both the GDPR and the MHMDA contain strong protections, they differ greatly in their core approach. While the GDPR strongly emphasizes the rights of individuals over their personal data, it lacks the specificity of the MHMDA when it comes to categorical protection of health information.

1. Overview

The GDPR has been hailed as the "toughest privacy and security law in the world."[129] It is broad in both substantive and territorial scope—its obligations extend to businesses anywhere that target or collect data from E.U. citizens[130]—but its regulations are not narrowly tailored.[131] In fact, while the GDPR is fairly restrictive, it is vague in many of its requirements, which experts have noted creates problematic uncertainty.[132]

Personal data, as protected by the GDPR, refers to "any information relating to an identified or identifiable natural person."[133] The GDPR only allows regulated entities to process personal data

---

128. 2016 O.J. (L 119).

129. Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR EU (last visited Mar. 2, 2026), https://gdpr.eu/what-is-gdpr [https://perma.cc/HCM3-9Z7V].

130. 2016 O.J. (L 119) art. 3.

131. *See* Wolford, *supra* note 129 ("The regulation itself is large, far-reaching, and fairly light on specifics.").

132. *See Top five concerns with GDPR compliance*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance [https://perma.cc/QJH9-F98S] (last visited Mar. 2, 2026) ("The lingering uncertainty around the GDPR is one of the biggest impediments to compliance, with parts of it deliberately left vague."); *see also* Shoshana Wodinsky, *The Hidden Failure of the World's Biggest Privacy Law*, GIZMODO (Feb. 4, 2022), https://gizmodo.com/gdpr-iab-europe-privacy-consent-ad-tech-online-advertis-1848469604 [https://perma.cc/N8PE-8A74] (discussing sanctions leveled against IAB Europe and compliance difficulties under the GDPR). Several provisions, such as the "undue delay" and "risk to rights" clauses, are difficult to interpret and have given businesses room to take liberties in their own interpretations. Mohammed Saqr, *Is GDPR failing? A tale of the many challenges in interpretations, applications, and enforcement*, 16 INT. J. HEALTH SCI. 1 (2022).

133. 2016 O.J. (L 119) art. 4(1).

under six enumerated circumstances.[134] Processing personal data is lawful under the GDPR when:[135]

- the consumer granted unambiguous consent;
- personal data processing was necessary to enter a contract with the consumer (i.e., a background check);
- processing was necessary to comply with a legal obligation (such as a court order).
- processing was necessary to save someone's life;[136]
- processing was necessary to perform an official function or serve the public interest; and
- the entity has a legitimate interest in processing personal data.[137]

Even with a legitimate purpose, the GDPR requires that regulated entities minimize their processing of personal data to only what is absolutely necessary.[138] The GDPR also identifies eight rights for consumers: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights related to automated decision making.[139]

"Data concerning health" is further defined as any personal data related to "the physical or mental health of a natural person, including the provision of healthcare services, which reveal

---

134. *Id.* art. 6.

135. *Id.*

136. This basis for processing personal data is reminiscent of the CCPA exception for emergency access to personal information where "a natural person is at risk." One key difference, however, is that the GDPR provides this as one required legal basis for the processing of data by a regulated entity itself, whereas the CCPA exception forced regulated entities to share this "life-saving" data with relevant agencies. If this was a current risk in the E.U., the GDPR provision would be less susceptible to abuse by groups seeking to criminalize abortion and funnel reproductive health information to law enforcement. All but two E.U. member countries have broadly legalized abortion. CTR. FOR REPRODUCTIVE RTS., EUROPEAN ABORTION LAWS: A COMPARATIVE OVERVIEW 2 (2023), http://reproductiverights.org/wp-content/uploads/2023/09/European-Abortion-Laws-A-Comparative-Overview-new-9-13-23.pdf [https://perma.cc/UXM6-GZJK].

137. 2016 O.J. (L 119) art. 6(1).

138. 2016 O.J. (L 119) art. 5(1)(c).

139. INFO. COMM'R'S OFF., A GUIDE TO INDIVIDUAL RIGHTS 7 (2025), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights [https://perma.cc/2SFR-42EM].

information about his or her health status."[140] Data concerning health is identified as a special category of personal data, and is granted additional protections under article 9.[141]

2. Differences in Health Data Protection

One pitfall of the GDPR's health data protection is its ambiguity relative to statutes like the MHMDA. The language is vague enough to leave definitional gray area as to what would be considered "health data."[142] Where the MHMDA outlines many specific forms of information included in the consumer health data umbrella,[143] the GDPR does not elaborate beyond the definition provided above.

Another apparent difference is that the MHMDA also recognizes that intimate health information can be inferred from non-sensitive data, and the statute accordingly prohibits these inferences from being derived and shared.[144] While this is not made explicit in the text of the GDPR, the Court of Justice of the European Union recently held that data from which sensitive inferences are drawn may itself be considered sensitive data under the GDPR.[145] A problem arising from this ruling, however, is that sensitive inferences can be derived from all sorts of data, and it is therefore unclear where the line will be drawn as to what is inference-producing data.[146] This is yet another issue of definitional uncertainty, which reduces regulatory predictability and creates difficulty for enforcement. The MHMDA sidesteps this problem by prohibiting the health-related inferences themselves, rather than the seemingly innocuous data from which they are derived.

The GDPR bans the processing of sensitive categories of personal data generally but outlines ten allowable legal bases for its collection and use.[147] By requiring an additional lawful basis for

---

140. 2016 O.J. (L 119) art. 4(15).

141. *See infra* notes 147–49 and accompanying text (detailing these additional protections).

142. 2016 O.J. (L 119) art. 4(15).

143. WASH. REV. CODE § 19.373.010(8) (2023).

144. *Id.* § 19.373.010(8)(b).

145. Case C-184/20, OT v. Vyriausioji tarnybinės etikos komisija, ECLI:EU:C:2022:601, ¶17–18 (Aug. 1, 2022).

146. *See* Daniel Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 NW. U. L. REV. 1081, 1103 (2024) (discussing how readily sensitive inferences can be made from nonsensitive data).

147. 2016 O.J. (L 119) art. 9(2).

sensitive data specifically, the GDPR in effect adds a second barrier to the collection and use of health information. These exceptions for sensitive data include instances of consent from the consumer where it is necessary for employment, social security, and protection of the consumer's "vital interests," as well as where the data was made publicly available, for charitable activities, legal claims, healthcare use, research, public interest and public health purposes.[148] Although this is a longer list of legal bases than the GDPR provides for personal data processing, this provision actually narrows the scope of allowable health data collection by excluding the broad "legitimate interest" basis, which companies are able to cite in order to collect non-sensitive personal data.[149] However, this provision still allows health data processing in more situations than the MHMDA, which requires either the consent of the consumer or strict necessity.

The GDPR's approach to protecting sensitive data has also faced criticism for its focus on creating a special category of data, seen as inherently deserving heightened protection. Intellectual property and technology law Professor Daniel Solove argues that this categorization is arbitrary, the lines are blurry, and the "sensitive data" label tracks harm poorly.[150] Instead, he proposes that the law focus on harm and risk rather than predefined categories.[151] The GDPR identifies a broad category of data that by its nature warrants privacy, whereas the MHMDA is closer to this risk-and-harm approach proposed by Solove. It precisely defines a form of data which faces specific risks in a post-*Dobbs* world, and seeks to limit the actual methods of collection and sharing which may lead to harm. This approach helps avoid the problems of vagueness and arbitrariness of the GDPR's sensitive data approach while targeting specific harm more directly.

3. A Rights-Based Model

Some of the more foundational differences between the GDPR and statutes like the MHMDA stem from a fundamental difference in approach. The GDPR is derived from a set of broader rights and principles. The E.U.'s conception of data privacy in the digital age is grounded in the idea that technological advancement must be anchored in the fundamental rights of individuals, which includes a

148. *Id.*
149. *Id.* art. 6(1)(f).
150. Solove, *supra* note 146, at 1111–27.
151. *Id.* at 1128–37.

sort of ownership over their personal information.[152] E.U. data privacy legislation developed out of an attempt to codify these broader ideals in specific provisions.[153]

While this approach may have contributed to some of the vagueness issues discussed above, it has resulted in a privacy scheme helpfully guided by a set of enumerated ideals. The GDPR lays out seven key principles that form the foundation of the statute and its provisions. These principles include fairness and transparency, lawfulness, purpose limitation, data minimization, accuracy, storage limitation, accountability, integrity and confidentiality.[154] All specific rules of the GDPR embrace these fundamental values, and adherence to the spirit of these values must guide both compliance and enforcement.[155] The MHMDA and other state statutes have no such guiding principles.

The E.U. has further acknowledged that in the digital age, any conception of a human right to privacy must also extend to digital spheres. Article 8 of the Charter of Fundamental Rights guarantees a right to protection of personal data.[156] One specific right stemming from this right to digital privacy is the right to be forgotten, which refers to an individual's affirmative right to request the erasure of their data.[157] This right was first established by the Court of Justice of the European Union in 2014, and was then encoded as one of the rights granted to consumers under the GDPR.[158] While the right to be

---

152. For a more in-depth treatment of the underlying differences between the American and European approaches to data privacy, *see* ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY (2023).

153. *See* 2016 O.J. (L 119) art. 1(2) ("This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.").

154. *Id.* art. 5(1).

155. Regulated entities are directed to demonstrate compliance with the spirit of these principles. *Id.* art. 5(2) ("The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1."). *See also id.* art. 4(7) ("'[C]ontroller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.")

156. Charter of Fundamental Rights of the European Union, art. 8(1), 2012 O.J. (C 326) 391, 397.

157. *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317, ¶¶ 89–99 (May 13, 2014) (creating and defining the right to be forgotten).

158. *Id.*; 2016 O.J. (L 119) art. 17.

forgotten is not recognized in the U.S. generally, the MHMDA also grants consumers the right to request the deletion of personal data.[159]

In the United States, privacy hinges on a right against intrusion by private or government actors, rather than on specific affirmative rights.[160] The GDPR's approach to affirmative privacy rights (and, broadly, the E.U.'s approach to digital privacy) establishes a foundation for more sweeping privacy protections. This rights-based approach could be embraced in jurisdictions where state constitutions have guaranteed more robust, affirmative privacy rights, further strengthening the legal basis for legislation seeking to protect health data.

III. PROPOSING A STATE-BASED MODEL OF PRIVACY PROTECTION

Despite widespread agreement among experts that federal data privacy legislation is needed, Congress has consistently refused to pass any federal data privacy law whatsoever. Attempts to do so—such as the American Data Privacy and Protection Act,[161] the Fourth Amendment is Not for Sale Act,[162] and the My Body My Data Act[163]—have all failed. There are many potential reasons for this, such as lobbying from the data industry, inability to agree and increased polarization within Congress, or concerns over preemption.[164] Regardless, the practical reality is that this is unlikely to change anytime soon. But there is a pressing need for data privacy protection right now, particularly in the realm of intimate health data. States do not have to wait for the federal government to address the issue. States can and should take initiative to protect the privacy of their residents, just as Washington has demonstrated is possible.

---

159. WASH. REV. CODE § 19.373.040(1)(c).

160. *See* Uta Kohl, *Right to be Forgotten and Two Western Cultures of Privacy*, 72 INT'L. & COMPAR. L.Q. 737, 754 (2023) (examining how differences in data privacy protection in the E.U. and in the U.S. stem from different conceptions of the right to privacy).

161. H.R. 8152, 117th Cong. (2022).

162. H.R. 4639, 118th Cong. (2023).

163. H.R. 8111, 117th Cong. (2022).

164. It appears that preemption concerns, as well as inability to resolve debates over data minimization and enforcement provisions, have stalled and halted development of federal data privacy legislation. *See* David Botero, *Federal privacy law: Analysis of comments to the US House privacy working group*, IAPP (Dec. 16, 2025), https://iapp.org/news/a/federal-privacy-law-analysis-of-comments-to-the-house-privacy-working-group [https://perma.cc/8BAA-VW6Y] (analyzing comments to the U.S. House data privacy working group).

The MHMDA, compared to other state privacy laws, currently provides the most robust example of health data protection.[165] Although more time is needed to see the full practical impacts of this legislation within the state of Washington, its language and provisions certainly appear to succeed in closing gaps left by other legislation to protect health information.[166] It therefore serves as an excellent model for the structure, language, and provisions other states should adopt if they are looking to address health data privacy concerns. Still, the MHMDA is not without its flaws. This Part examines the MHMDA more closely to identify problematic elements that should be eliminated or addressed in future efforts at developing similar privacy legislation.

A. Criticisms of the MHMDA

One potential problem is that the breadth of the MHMDA's provisions can create some ambiguity as to what is properly regulated under the statute. While its contours are not as vague as the GDPR's, there are still some uncertainties that are likely to invite litigation. For instance, the MHMDA includes a sweeping definition of data "collection," which means "to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner."[167] The scope of this definition may be unclear in practice. Does accessing or receiving health data while merely traveling through Washington count as collection? If a company uses an artificial intelligence (AI) system based in Washington to derive

---

165. The merit of the MHMDA as a model for future health privacy legislation has been acknowledged at the federal level. United States Representative Sara Jacobs introduced the My Body, My Data Act in 2022, modeled off the MHMDA, in the hopes of establishing specific protections for individual reproductive health information. *See* My Body, My Data Act, H.R. 8111, 117th Cong. (2022). This bill, unfortunately, was not passed. Senators Hirono and Wyden attempted to reintroduce Representative Jacobs's Act in 2023, but it did not pass the Senate either. My Body, My Data Act, S. 1656, 118th Cong. (2023); *see also* Press Release, Senator Ron Wyden, Sens. Wyden, Hirono, Rep. Jacobs Reintroduce the My Body, My Data Act to Protect Reproductive and Sexual Health Data (May 18, 2023), https://www.wyden.senate.gov/news/press-releases/sens-wyden-hirono-rep-jacobs-reintroduce-the-my-body-my-data-act-to-protect-reproductive-and-sexual-health-data [https://perma.cc/NE2N-Q26G] (highlighting comments from the Senators and Representative Jacobs on the need for online reproductive health privacy). The repeated failure of the My Body, My Data Act reflects the unfortunate reality that the United States is unlikely to see federal health data privacy protections in the near future.

166. *See supra* Part II (comparing the MHMDA to CCPA and the GDPR).

167. WASH. REV. CODE § 19.373.010(5) (2023).

consumer health information, but does its actual business and data collection outside of the state, is it regulated by the MHMDA?[168] The answers to these questions, based purely on the plain language of the statute, appear to be yes—any person whose health data is "collected in Washington" is considered a protected consumer, meaning any data processing in Washington may implicate a company.[169] Under the language of the statute, virtually any entity whose health data touches the state could be subject to compliance, but courts may not uphold application of the statute where the company does not have a significant nexus to the state.[170] Washington courts have yet to see any litigation on the matter, making it difficult to predict where the line will be drawn.

This can make it difficult for businesses to navigate compliance on the front end, a dynamic that is further complicated by the risk of class action litigation. The private right of action established under Section 11 of the MHMDA is uniquely far-reaching.[171] Any violation of the statute is considered an unfair or

---

168. *See* Jenny Colgate, *Wash. Health Privacy Bill May Affect Cos. Across Industries*, LAW360: EXPERT ANALYSIS (July 6, 2023), https://www.law360.com/articles/1695726/wash-health-privacy-bill-may-affect-cos-across-industries (on file with the *Columbia Human Rights Law Review*) (discussing the potential for the MHMDA to cause "more privacy litigation than we have seen under any other state privacy statute to date").

169. Washington courts have not yet engaged in any statutory interpretation for the MHMDA, so it remains to be seen whether courts will read implied limitations into this provision. *See* Mike Hintze, *The Washington My Health, My Data Act: Not Just Washington (Or Health)*, CAL. LAWS. ASS'N (May 2, 2024), https://calawyers.org/privacy-law/the-washington-my-health-my-data-act-not-just-washington-or-health [https://perma.cc/J7P8-LLLN] (noting that it remains unclear how courts will interpret the Act and companies should account for potential risks in creating compliance strategies).

170. There is potential for courts to find that such a broad reading exceeds the state's authority to regulate interstate commerce. *See infra* Part III.B. Under the Dormant Commerce Clause, a state generally may not regulate commercial activity which takes place entirely outside the state. *See* South Dakota v. Wayfair, Inc., 585 U.S. 162, 177–78 (2018) (holding that the Dormant Commerce Clause does not prohibit states from collecting sales taxes from internet retailers without a physical presence in the state).

171. *See* Andreas Kaltsounis & Alexander Vitruk, *Examining the Private Right of Action in Washington's My Health My Data Act*, BAKER & HOSTETLER (July 19, 2023), https://www.bakerdatacounsel.com/blogs/examining-the-private-right-of-action-in-washingtons-my-health-my-data-act [https://perma.cc/VYP3-9BE8] (discussing the uniquely extensive scope of the MHMDA's private right of action). It is also uncertain whether a claim accrues only once at the company's first instance of violation against the plaintiff, or whether additional claims accrue with each instance of prohibited data collection or sale, as is the case with

deceptive act under the Washington Consumer Protection Act, allowing for private plaintiffs to bring litigation against any regulated entities.[172] The MHMDA includes no opportunity to cure, does not limit actions by severity of violation or procedural posture, and it does not impose a minimum harm threshold.[173] Experts have noted that this may lead to a plethora of nuisance claims that do not meaningfully advance the MHMDA's privacy goals.[174] The previously discussed uncertainties surrounding application of the MHMDA's "broadly defined" terms add to this by opening the door to attempts by plaintiffs to stretch the statutory definitions.[175] The pool of potential plaintiffs is additionally expanded by the statute's broad definition of consumer.[176] And while there are no statutory damages under the Washington Consumer Protection Act, it provides for actual damages and attorneys' fees, creating incentives that generate an unusually high risk of class action lawsuits for regulated entities.[177] Because harm need not be monetary, a large injured class could be easily identified.[178]

Illinois' Biometric Information Privacy Act. *Id.*; *see also* Biometric Privacy Act, 740 ILL. COMP. STAT. 14/15 (2008) (codifying an individual's right to privacy in and control over their biometric identifiers and biometric information); Cothron v. White Castle Sys., Inc., 477 F. Supp.3d 723, 731–32 (N.D. Ill. 2020) ("A party violates [the Illinois Act] when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with *each* subsequent scan or collection." (emphasis added)).

172. WASH. REV. CODE § 19.373.090 (2023).

173. *See id.* (lacking these elements).

174. *See* Kaltsounis & Vitruk, *supra* note 171.

175. *See* Colgate, *supra* note 167.

176. WASH. REV. CODE § 19.373.010(7) (2023). 'Consumer' is defined as "a natural person" who either is a Washington resident or whose consumer health data is collected in Washington, and who "acts only in an individual or household context." *Id.* An individual acting in an employment context is not defined as a consumer. *Id*.

177. WASH. REV. CODE § 19.138.280 (1994).

178. Privacy and cybersecurity law Professor Mason Clark posits that the private right of action should be both limited and fortified to remedy these issues. Mason R. Clark, *Consumer Privacy and the* Dobbs *Disruption*, 58 U. MICH. J.L. REFORM 1, 5–6 (2024). Specifically, he argues that claims should be limited to instances where a regulated entity shared health data with a government agency, law enforcement, or other regulatory body, and that disclosing data to these entities should be an injury *per se*. *Id.* at 60–61. However, this approach would greatly hamper the MHMDA's ability to regulate the data broker market, as it would prevent enforcement of data sharing regulations where intimate data is being shared and sold among private parties.

The difficulty of compliance with the MHMDA runs the risk of deterring companies and other entities from doing business within the state. Not only does it impose a significant regulatory burden,[179] but it also carries a high risk of litigation. Companies must weigh the costs of adjusting their operations to align with a stricter interpretation of the statute's regulations against the potential costs of litigation should their interpretation of the statute's requirements fall short in any way. This can't be ignored by legislators; the strength of any privacy law's protections must be balanced against the feasibility of compliance. But the benefit of a stricter regulatory approach is that it incentivizes early preparation and ongoing compliance efforts among entities seeking to do business with the state. If such protections become popular among many states, this could simply become the new norm for companies that handle data, protecting consumers even outside the states that impose these requirements.[180]

B. Potential Legal Challenges

The MHMDA was implemented too recently to be the subject of any litigation, and similar privacy statutes like the CCPA have yet to be challenged under legal bases that could be applicable to the MHMDA.[181] While this bodes well for the MHMDA, there is still one

---

179. Affirmative consent obligations and other requirements set by the statute will impose additional costs and compliance burdens on businesses. *See, e.g.*, WASH. REV. CODE § 19.373.030 (2023) (requiring consumer authorization for health data collection and sharing).

180. This effect is observable through the GDPR itself. The GDPR, like the MHMDA, targets any companies that do business with residents of the E.U. 2016 O.J. (L 119) art. 3(2). As a result, any businesses worldwide that want to do business with residents of the E.U. must comply with its data privacy requirements. The E.U. is a large enough market to incentivize compliance by businesses globally. *See* Jennifer Wu & Martin Hayward, *International impact of the GDPR felt five years on*, PINSENT MASONS (May 25, 2023), https://www.pinsentmasons.com/out-law/analysis/international-impact-of-the-gdpr-felt-five-years-on (on file with the *Columbia Human Rights Law Review*) (discussing the GDPR's impact on both policymaking and business data protection practices internationally). A single state like Washington likely would not be enough to inspire widespread data privacy compliance in the private sector, but if enough states implement similar legislation, U.S. businesses will face pressure to comply if they do not wish to lose access to a substantial portion of the market.

181. Recent challenges to California privacy laws have not focused on issues relevant to the MHMDA. *See* California Priv. Prot. Agency v. Sup. Ct. of Sacramento Cnty., 99 Cal. App. 5th 705, 711 (Cal. Ct. App. 2024) (addressing the date of the Agency's authority to enforce regulations); NetChoice, LLC v. Bonta,

area where the statute may be predicted to run into trouble—the Dormant Commerce Clause.[182]

The strongest basis for challenging the MHMDA would be a claim that it violates the Dormant Commerce Clause. This doctrine imposes a limitation on state authority to regulate or unduly burden interstate commerce, since this power is held exclusively by Congress.[183] State laws that discriminate against out-of-state entities or regulate activity that happens entirely outside the state may therefore be prohibited.[184] A central goal of this doctrine is to "prevent[] the States from adopting protectionist measures."[185] The MHMDA regulates any out-of-state entities that conduct business with or target consumers in Washington, not limited by physical presence in the state.[186] While the Dormant Commerce Clause does not limit regulatory activity to businesses that are physically present in the state,[187] due to the nature of online activity there is a high likelihood that the MHMDA will encompass entities that have only *de minimis* contacts with Washington. This leaves the door open to arguments that the MHMDA reaches entities that do not have a sufficient nexus to the state, in violation of the Dormant Commerce Clause.

When assessing Dormant Commerce Clause claims, courts must first consider whether a statute is discriminatory "either on its

---

113 F.4th 1101, 1108 (9th Cir. 2024) (enjoining a California statute that imposed requirements on websites likely to be accessed by children because it was in violation of the First Amendment).

182. U.S. CONST. art. 1, § 8, cl. 3.

183. Cong. Rsch. Serv., *Artl.S8.C3.7.1 Overview of Dormant Commerce Clause*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/artI-S8-C3-7-1/ALDE_00013307 (on file with the *Columbia Human Rights Law Review*) (last visited Mar. 24, 2026).

184. *See* South Dakota v. Wayfair, Inc., 585 U.S. 162, 177–78 (2018) (holding that the Dormant Commerce Clause does not prohibit states from collecting sales taxes from internet retailers without a physical presence in the state).

185. Tennessee Wine & Spirits Retailers Ass'n v. Thomas, 588 U.S. 504, 514 (2019) (finding that state law provisions imposing demanding residency requirements for a license to operate a liquor store violate the Commerce Clause); *see also* Baldwin v. G. A. F. Seelig, Inc., 294 U.S. 511, 527 (1935) ("What is ultimate is the principle that one state in its dealings with another may not place itself in a position of economic isolation.").

186. WASH. REV. CODE § 19.373.010(23).

187. *Wayfair*, 585 U.S. at 184–87 (overruling the physical presence rule and recognizing that the internet has "changed the dynamics of the national economy").

face or in practical effect."[188] This analysis must be context-based and case-specific; there is no bright-line rule for what meets the level of discriminatory purpose or effect required.[189] Statutes that evenhandedly regulate both in-state and out-of-state businesses will generally be upheld.[190] If a court finds that a statute is discriminatory, the burden shifts to the state to justify its potential effects by establishing it meets two standards.[191] First, the state must show that the statute "serves a legitimate local purpose."[192] Second, the state must show that the statute's local purpose could not be served as well by nondiscriminatory means.[193]

The MHMDA is not facially discriminatory, as it imposes the same compliance standards on both in-state and out-of-state businesses.[194] It also cannot be said to have a discriminatory purpose, as its purpose is to protect the privacy of Washington residents from all businesses that may harvest intimate data.[195] There are no indications of a direct intent to impede interstate commerce or drive away out-of-state competitors. The mere fact that the MHMDA's regulations reach businesses not physically located in Washington does not put it in violation of the Dormant Commerce Clause.[196] But Courts may still find that the MHMDA has a discriminatory effect through essentially prohibitive regulations. Although the MHMDA holds all businesses that deal with Washington residents to the same

---

188. Hughes v. Oklahoma, 441 U.S. 322, 336 (1979).

189. *See* West Lynn Creamery, Inc. v. Healy, 512 U.S. 186, 201 (1994) (noting that Commerce Clause jurisprudence has "eschewed formalism for a sensitive, case-by-case analysis of purposes and effects").

190. *See* Minnesota v. Clover Leaf Creamery Co., 449 U.S. 456, 470 (1981) (finding that a statute prohibiting retailers from selling milk in plastic containers was nondiscriminatory and served a substantial state interest in reducing solid waste).

191. *See, e.g.*, Maine v. Taylor, 477 U.S. 131, 138 (1986) (finding that protecting native fisheries was a legitimate local purpose that could not be served as well by nondiscriminatory means).

192. *Id.*

193. *Id.*

194. WASH. REV. CODE § 19.373.010(3) (2023) (defining "regulated entity" to include any business that targets Washington consumers, whether located in Washington or not).

195. *Id.* § 19.373.005.

196. *See* South Dakota v. Wayfair, Inc., 585 U.S. 162, 184–87 (overruling the physical presence rule); *see also* Rocky Mountain Farmers Union v. Corey, 913 F.3d 940, 952 (9th Cir. 2019) ("[S]ubjecting both in and out-of-jurisdiction entities to the same regulatory scheme to make sure that out-of-jurisdiction entities are subject to consistent environmental standards is a traditional use of the State's police power").

standards, the regulatory burden it imposes is heavy due to its affirmative consent obligations and other provisions.[197] The cost of compliance for businesses that do not do a substantial amount of business with Washington residents may outweigh any profit they receive from doing business within the state. It could therefore have the effect of driving away out-of-state businesses that cannot afford to bear that burden.

Despite this, Courts are not likely to strike down the MHMDA. Although the statute's requirements do impose a burden on interstate commerce, this burden is justified by its legitimate purpose. Protecting the data privacy of Washington residents is a compelling interest that the state has clearly indicated its intent to prioritize.[198] The regulations imposed by the MHMDA create a clear, strong local benefit to Washington residents: the protection of their privacy and autonomy with regard to their most intimate health information. The fact that the MHMDA narrows its focus to health data bolsters the argument for its strong local benefit—it is specified and well-defined, not some vague notion of privacy.[199] Further, courts are not likely to strike down the MHMDA on the grounds that its aims could be achieved by alternative, less restrictive means. While it is possible to construct a less restrictive version of this statute, every provision stricken from the statute sacrifices a key piece of privacy protection. Lessening the regulatory burden would, in this case,

---

197. *See, e.g.*, WASH. REV. CODE § 19.373.030 (2023) (requiring consumer authorization for health data collection and sharing).

198. *Id.* § 19.373.005.

199. The Court has at times applied a more deferential balancing test when evaluating a potential Dormant Commerce Clause violation. Under this test, the Court assesses the burden imposed on interstate commerce by a state law and prevents its enforcement if the law's burdens are "clearly excessive in relation to the putative local benefits." Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970). Though this balancing test has not been formally overruled, it has largely fallen out of use in favor of the modern test employed by the Court in *Hughes* (and applied in this section). Hughes v. Oklahoma, 441 U.S. 322, 335–36 (1979). Specifically, the Court has held that the *Pike* test should only be used where the variables to be balanced are directly comparable. *See* National Pork Producers Council v. Ross, 598 U.S. 356, 380–83 (2023) (plurality) (noting that the comparison of economic cost to human treatment was "incommensurable"). Here, the human and dignitary benefits of health privacy cannot be fully measured against the related economic costs. Still, if the *Pike* balancing test were applied, the MHMDA would likely prevail for many of the reasons discussed in this paragraph. Though a burden is undoubtedly imposed by the statute, it is not so excessive as to outweigh the clear local benefits of increased health data privacy achieved by the MHMDA.

result in a less comprehensive set of privacy protections that ultimately fail to serve the state's legitimate purpose as well.[200]

Courts may also attempt to avoid Commerce Clause concerns altogether through a narrower interpretation of the MHMDA's scope. Holding that it only regulates businesses with a sufficient nexus to the state and its residents could greatly reduce or eliminate the problem of a potential interstate discriminatory effect. The downside is that this could create gaps in the protection of Washington residents, just by virtue of the fact that not all businesses dealing with residents would be regulated. This tradeoff may be undesirable, and even unnecessary, given the arguments outlined above. Regardless, other privacy statutes following the MHMDA's model are likely to overcome a challenge under the Dormant Commerce Clause. In order to ensure this, such a statute should be similarly focused on health data privacy, clearly state its intended impact on the privacy of the state's residents, and avoid placing an unrealistically high regulatory burden on businesses with minimal state contacts.

C. Additional Recommendations

There are other ways in which a statute emulating the MHMDA could be strengthened, whether through the language of the statute itself or through accompanying legislation. Several scholars discussed in this Section have pointed out specific elements needed to ensure regulations are creating an effective data privacy framework—one that does not contain any significant gaps for data brokers or government entities to take advantage of.

1. Park's Three Corners of Privacy

Privacy law Professor Eunice Park suggests that to properly address reproductive privacy concerns, there are "three corners" of data protection that must be secured through data privacy

200. Courts have also traditionally held that a company is not entitled to its "preferred method of operation." Exxon Corp. v. Governor of Maryland, 437 U.S. 117, 127–28 (1978) (finding that the Dormant Commerce Clause "protects the interstate market, not particular interstate firms, from prohibitive or burdensome regulations"). Requiring out-of-state businesses to change their data collection and retention methods falls within the level of regulatory burden states have the authority to impose, so long as they are justified by a legitimate interest.

legislation.[201] Two of these corners can be effectively addressed by state legislation like the MHMDA. The first "corner" is the inclusion of a specific carve-out for reproductive information within its definition of healthcare data.[202] The MHMDA specifically names sexual and reproductive health data as a form of protected healthcare, which distinguishes it from other data privacy statutes.[203]

The second "corner" Park identifies as necessary is banning data brokers from selling health data to law enforcement.[204] The MHMDA accomplishes something similar by prohibiting the sale of health data without the separate informed consent of the consumer.[205] Even though law enforcement is still allowed to purchase data under the MHMDA, regulated entities must disclose the intended recipient of any health data sale.[206] This informed consent process ensures that consumers consent to the disclosure of their health data to law enforcement, which mimics the requirement that individuals consent to warrantless searches by law enforcement.[207] A total ban on the sale of health data would perhaps more thoroughly close the gaps left by HIPAA and the Fourth Amendment, as this would prevent health data from entering the data market on the front end, thereby preventing any further sharing and transfer. Still, the MHMDA's informed consent requirements significantly protect against existing loopholes.

Park's third corner, however, is an additional procedural safeguard that the MHMDA does not address. Park argues for federal legislation barring the use of reproductive health data obtained without a warrant as the basis for prosecution;[208] such a requirement

---

201. 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).

202. *Id.* at 253–54.

203. *See supra* Part II.A (comparing the MHMDA to the CCPA).

204. Park, *supra* note 201, at 260–65.

205. WASH. REV. CODE §§ 19.373.030, 19.373.070 (2023).

206. *Id.*

207. Consent is a long-established exception to the Fourth Amendment warrant requirement. Davis v. United States, 328 U.S. 582, 593–94 (1946); Zap v. United States, 328 U.S. 624, 630 (1946).

208. Park, *supra* note 201, at 265–67. Park argues that "the 'third corner' warrant requirement for reproductive health data should encompass all the mechanisms through which law enforcement can obtain identifiable data without probable cause: subpoena or order; law enforcement surveillance technology; and general data collection . . . . This approach ensures that all methods, traditional and otherwise, are Fourth Amendment searches when the data is sought to criminalize abortion or related services . . . ." *Id*. at 269.

could close any loopholes used by law enforcement to obtain health data without probable cause. States looking to implement privacy legislation cannot count on a federally mandated warrant requirement, but a state legislature could enshrine such a warrant requirement in state law.[209] This is a gap that Washington's data privacy statutes do not address.

In practice, this could be operationalized through a statute barring state governmental entities from obtaining individual health data without a proper judicial warrant.[210] Montana recently became

---

209. State high courts also have the authority to interpret their state constitutions to be more protective than the Fourth Amendment. *See* G. Alan Tarr, *The Past and Future of the New Judicial Federalism*, 24 PUBLIUS: J. FEDERALISM 63 (1944) (discussing the development of the new judicial federalism, which has enabled increased reliance on state constitutions to expand rights beyond the minimum guaranteed under the federal constitution). This authority can only be forfeited if a state legislature explicitly provides that the state will be in lockstep with federal Fourth Amendment jurisprudence. Stephen Henderson, *States in 'Lockstep' with the Fourth Amendment May Not Be Locked*, STATE CT. REP., (Aug. 12, 2024), https://statecourtreport.org/our-work/analysis-opinion/states-lockstep-fourth-amendment-may-not-be-locked [https://perma.cc/A8MJ-ZSQP]. For example, the Florida legislature added a provision to its constitution's search and seizure protection stating that "[t]his right shall be construed in conformity with the 4th Amendment to the United States Constitution, as interpreted by the United States Supreme Court." FLA. CONST. art. I, § 12 (amended 1982); *see also* State v. Creller, 386 So. 3d 487, 492 (Fla. 2024) (where the Court acknowledges "we are constitutionally bound on search and seizure issues to follow the decisions of the United States Supreme Court"). Even still, the Florida constitution contains additional privacy provisions that the Florida Supreme Court has used to establish protections beyond the Fourth Amendment within the state. *See* FLA. CONST. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."); Shaktman v. State, 553 So. 2d 148, 151 (Fla. 1989) (finding that this right to privacy under the Florida Constitution was implicated by the government's use of a pen register to gather phone numbers, even though this information was possessed by a third party telephone company). California's rights related to suppression of evidence are also in lockstep with federal Fourth Amendment jurisprudence thanks to its "Truth-in-Evidence" constitutional provision, which was also added in 1982. *See* CAL. CONST. art I, § 28 (1982). This reality highlights the importance of the legislature's participation in expanding privacy protections.

210. It must be noted that this approach comes with a significant limitation: such a statute would only govern the law enforcement of the state which enacts it. The states that are interested in employing these measures to protect reproductive health data are unlikely to be criminalizing and prosecuting abortion. Still, codifying these protections will protect against changing politics and shape law enforcement behavior. Additionally, even anti-abortion states may see value in protecting health data generally, and political will for a warrant

the first state to close the data broker loophole through such a statute by banning the purchase of data.[211] This statute is sweeping in its protections, which encompass not just "sensitive data,"[212] but also geolocation data and the contents of electronic communications.[213] States looking to codify a similar warrant requirement should more closely define the health data receiving heightened privacy protection, and should also include provisions which prevent the government from obtaining health data from entities with misleading privacy policies.[214] Though a statute like the MHMDA should ideally prevent companies from engaging in shady privacy practices, the additional procedural safeguard can prevent harm to affected users when companies fail to comply with regulations.[215]

2. Prince's Four Key Elements

Health privacy law Professor Anya Prince argues that health data privacy legislation must include four key elements to be truly comprehensive.[216] First, it must regulate data brokers.[217] The private health data market not only enables invasive marketing tactics by advertisers, but it also allows law enforcement agencies to purchase

---

requirement could materialize in these states as these statutes become the norm elsewhere.

211. Matthew Guariglia, *Montana Becomes First State to Close the Law Enforcement Data Broker Loophole*, EFF (May 14, 2025), https://www.eff.org/deeplinks/2025/05/montana-becomes-first-state-close-law-enforcement-data-broker-loophole [https://perma.cc/Q7Z2-84EY].

212. Defined under Montana law as "data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, information about a person's sex life, sexual orientation, or citizenship or immigration status," as well as biometric identifiers and precise geolocation data. Consumer Data Privacy Act, MONT. CODE ANN. § 30-14-2802(28) (2025).

213. MONT. CODE ANN. §§ 46-5-112, 46-5-602 (2025).

214. *See* Bhatia, *supra* note 7, at 95–100 (recommending changes to the failed Fourth Amendment is Not for Sale Act that would more effectively close this loophole).

215. Professors Aziz Huq and Rebecca Wexler argue for an even more absolute protection—statutory evidentiary privileges for reproductive health data. Aziz Huq & Rebecca Wexler, *Digital Privacy for Reproductive Choice in the Post-Roe Era*, 98 N.Y.U. L. REV 555, 634 (2023). While this would protect intimate health data from law enforcement even in the event a warrant was obtained, an absolute privilege comes with its own risks, and state legislatures may not be willing to take such an extreme measure.

216. Anya E.R. Prince, *Reproductive Health Surveillance*, 64 B.C. L. REV. 1077, 1135 (2023).

217. *Id.*

data for use in investigation and criminal prosecution.[218] The MHMDA accomplishes this indirectly by limiting health data sales to instances of informed consent,[219] although the ability of initial purchasers to then resell data without consent leaves a gap for the data broker market to exploit. A total ban on the sale of health data would likely better address the problem posed by data brokers by eliminating the potential for profiting from intimate health information.

Second, according to Prince, health data privacy legislation must protect inferences drawn from non-health data.[220] Failure to do so would leave a large gap; companies have access to sophisticated predictive algorithms, which allow them to infer health conditions and then sell that information to third parties.[221]

Third, it must include "upstream regulation"—provisions which maximize privacy protection by limiting the initial collection of health data on the front end.[222] The MHMDA addresses these two elements by explicitly including health inferences as protected health data and limiting collection and sharing of health data to instances of necessity or direct consent from the user.[223] However, it could do even more to enforce data minimization. A use-based data minimization mandate, for example, would ensure that regardless of consumer consent, only data that is reasonably necessary to provide the relevant product or service is collected.[224] Instead of allowing data collection based on consent *or* necessity, as the MHMDA does,[225] a consent requirement could be accompanied by a mandate that collection be limited by necessity in all instances. Additionally, requiring encryption and stricter data retention policies would further ensure that there is less data available to obtain by warrant or subpoena.

---

218. *See id.* at 1110–14 (discussing law enforcement's access to health data brought about by the monetization and sale of personal information).

219. WASH. REV. CODE § 19.373.070.

220. *See* Prince, *supra* note 216, at 1136.

221. *See supra* Part I.A. (describing how companies obtain and sell consumer health information).

222. Prince, *supra* note 216, at 1138.

223. WASH. REV. CODE §§ 19.373.030, 19.373.010(8)(b) (2023).

224. *See* Daniel Solove, *Privacy in Authoritarian Times: Surveillance Capitalism and Government Surveillance*, 67 B.C. L. REV. 51, 108 (2026) (recommending a use-based data minimization approach).

225. WASH. REV. CODE § 19.373.030(1)(b) (2023).

Prince also suggests that prohibiting regulated entities from "profiling" an individual's health could further limit the collection of reproductive health information from seemingly unrelated data.[226] This would provide protection beyond just the prevention of direct sharing—it would prevent data brokers from identifying profitable categories for advertising and thereby address the primary source of this market's profitability. A state looking to implement a statute similar to the MHMDA should consider adding a provision banning this sort of data aggregation in order to further strengthen reproductive health privacy.[227]

Unfortunately, Prince's fourth key element is a significant gap that the MHMDA is unable to fill. Prince argues that there must be consistent regulation across states, necessitating a federal solution.[228] One reason is that the individuals most in need of reproductive health data protection are the ones living in states that are unlikely to legislate reproductive health privacy.[229] Another is that, in cross-border abortions, an unprotected state will not limit the use of reproductive health data collected in (and targeting residents of) that state, even if the individual has travelled to a state like Washington for care.[230] Unfortunately, this could not be addressed through even the strongest data privacy law if that law is only passed in a single state. However, if enough states enact MHMDA-style legislation, most entities would have to comply with such state regulations in practice. Any business could forfeit too much of its consumer base if it was forced to stop engaging with residents of even a third of the states.[231] It would also be nearly impossible for online entities to entirely avoid contact with residents of regulated states. At that point, the costs of compliance would be thoroughly outweighed

---

226. *See* Prince, *supra* note 216, at 1138.

227. Recently, the Trump administration announced plans to engage in unprecedented centralized data aggregation within the federal government. Frenkel & Krolik, *supra* note 10. This would involve using Palantir in key federal agencies to merge all data the government has compiled on individuals within the country, effectively creating a database of U.S. citizens that would magnify the government's surveillance power. *Id.* While states cannot control what data their residents have handed over to the federal government itself through interactions with various agencies, banning the creation of additional data dossiers by corporations would help limit the amount of data available for collection by the federal government. Such a step is more important now than ever.

228. *See* Prince, *supra* note 216, at 1140.

229. *Id.*

230. *Id.*

231. *See supra* note 180 (discussing how the GDPR has influenced international data practices through a similar mechanism).

by the loss of business through failure to comply. These standards for health data privacy could become the new standard operating procedure across most entities that deal with data as a result.[232]

There is also a strong possibility that the landscape analyzed by Prince will change. In the event of a federal abortion ban, residents of states like Washington that currently protect the legal right to choose may find themselves at risk of federal prosecution.[233] Should that come to pass, MHMDA-style privacy legislation may be one of the few options available to states that seek to protect the right to privacy and autonomy over individual reproductive health.

CONCLUSION

Regulating data privacy will have impacts far beyond just protecting reproductive health information. As algorithms and data analysis grow more sophisticated, as the AI industry grows and feeds on available data, and as more of our personal lives and information find their way into the digital sphere, allowing the free sharing and reuse of our most intimate information will enable increasingly concerning privacy invasions.[234] Other human rights are at stake.

---

232. Another potential, albeit less likely, benefit of states leading the way in implementing these data protections is that it could provide support for future attempts to establish data privacy as a protected right. The Court has looked to state consensus as evidence for or against the existence of certain rights. Washington v. Glucksberg, 521 U.S. 702, 710–11 (1997) (finding that nationwide consensus weighs against assisted suicide as a right). However, the Court concurrently emphasized the long history of such a consensus. *Id.* Recently, current statewide consensus was far less important to the Court than historical consensus in their analysis of the abortion issue. Dobbs v. Jackson Women's Health Organization, 597 U.S. 215, 217 (2022) ("Indeed, abortion had long been a crime in every single state . . ."). There is no long history of health data protection in the United States. Still, a strong nationwide pattern of state privacy legislation could help lay the groundwork for future recognition of data privacy as a right.

233. A federal abortion ban was introduced in the House in January 2025. *See generally* Life at Conception Act, H.R. 722, 119th Cong. (2025) (vaguely protecting the right to life from fertilization). While it has not passed the House at the time of writing, a federal ban is certainly not out of the question given the current Republican majority in Congress. Such a ban would render state-level health data privacy protections even more essential. Even though it is unlikely state legislation could block federal subpoenas, limiting the collection of reproductive health data on the front end, as well as prohibiting inferences and data aggregation, could ensure there is less data available for law enforcement to seize.

234. *See* Mikayla Domingo, Note, *One Nation, Under Dobbs: How Dobbs v. Jackson Women's Health Impacts Data Privacy for All*, 15 U.C. L. SCI. & TECH. J.

Fears about inferences drawn from even the simplest online searches and posts can chill the exercise of free speech.[235] The same geofencing technology used to tie women to abortion clinics can be used to locate individuals at protests.[236] The surveillance already employed for commercial purposes can increasingly be taken advantage of by law enforcement and other government entities to identify and target specific demographics.[237]

Implementing comprehensive data privacy protection statutes state by state, with key provisions modeled off of the MHMDA, is the first step to counteracting these invasions. Such a statute should require informed consent for the collection of any health data and should grant consumers a right to delete their intimate data. It should include a similarly detailed definition of health data, as opposed to the ambiguous definition of the CCPA or the blurry sensitive personal data category of the GDPR.[238] This definition should specifically identify sexual and reproductive health information as protected and should also give equal protection to the health-related inferences drawn from non-health data. These definitional elements go a long way in eliminating uncertainty and ensure that there are no gaps for data brokers to take advantage of.

There are a few ways in which states should diverge from Washington's approach to further strengthen the health data privacy framework. Data collection should be defined more narrowly to

---

35, 35 (2024) ("[T]he exploitation of such personal data to target women seeking an abortion sets a precedent that will allow countless other groups to have their personal data exploited for whatever their state deems to be a 'legitimate government interest.'").

235. *See* Leila Nasrolahi, Note, *Data Surveillance and Abortion Bans After Dobbs*, 38 BERKELEY TECH. L. J. 1341, 1362–64 (2023) (discussing the chilling effects digital surveillance will have on not only legal reproductive healthcare, but also on information sharing).

236. U.S. Immigration and Customs Enforcement (ICE) has begun harvesting sensitive location data to track and surveil anti-ICE protestors as well as potential targets for immigration enforcement. Anika Venkatesh & Lauren Yu, *DHS is Circumventing Constitution by Buying Data It Would Normally Need a Warrant to Access*, ACLU (Jan. 12, 2026), https://www.aclu.org/news/privacy-technology/dhs-is-circumventing-constitution-by-buying-data-it-would-normally-need-a-warrant-to-access [https://perma.cc/EE9N-8U4Y].

237. This past year, ICE has used the same loopholes surrounding data privacy discussed in this Note to surveil and systematically target immigrants and people of color. *Id.* This demonstrates the potential of the commercial data collection structure to be weaponized by the government against other groups, not just those seeking reproductive healthcare.

238. CAL. CIV. CODE § 1798.140(v)(1); 2016 O.J. (L 119) art. 9(2).

increase certainty over what triggers compliance requirements. While the breadth of the MHMDA's protection in this regard seems desirable—on its face, preventing as much data collection as possible seems to be a great step towards protecting data privacy—it risks attempting to regulate entities that do not have sufficient nexus to the state. Defining this more carefully would clarify the scope while making the statute less susceptible to legal challenge. Data minimization should be further enforced through mandated use-based limitations and a universal consent requirement; this will ensure less personal data is collected in the first place and will prevent companies from obtaining health information without the consumer's direct knowledge and authorization. Finally, the sale of health data should be banned entirely to eliminate the profit incentive that leads to third party exploitation of sensitive personal data.

States should also consider adopting additional protections alongside an MHMDA-style health data statute. A statute or provision prohibiting governmental entities from obtaining health data evidence without a warrant would add a layer of procedural protection that could prove particularly important in safeguarding reproductive health information. A statute or provision prohibiting the health profiling of individual users could prevent predatory advertising by entities who do receive a user's permission to collect health data; this would also ensure there is no physical condition profile to be leaked, subpoenaed, or in any way released to third parties.

Finally, state constitutions can and should be amended to include an affirmative right to data privacy. Such an amendment would ensure that as technology evolves and new methods of data exploitation are developed, states still have an affirmative obligation to take action to preserve data privacy. The E.U. has acknowledged data privacy as an important human right in the digital age. Taking this step in the United States can help prevent other data concerns—invasions of personal privacy that we can't even contemplate yet—from creating real personal harm as technology continues to evolve.