

REPRODUCTIVE HEALTH SURVEILLANCE

ANYA E.R. PRINCE

INTRODUCTION	1078
I. THE REPRODUCTIVE HEALTH DATA ECOSYSTEM.....	1085
<i>A. Reproductive Health Information Sharing</i>	1086
1. Direct Information Sharing.....	1086
2. Indirect Information Sharing	1089
<i>B. Monetizing the Reproductive Health Data Ecosystem</i>	1091
1. Targeted Advertising and Harms.....	1092
2. Other Harms	1094
3. Inequitable Impacts	1095
<i>C. Privacy Regulation (or a Lack Thereof)</i>	1096
II. THE CHANGING REPRODUCTIVE HEALTH LANDSCAPE	1101
<i>A. Medical Landscape</i>	1101
1. Medication Abortion	1101
2. Assisted Reproductive Technologies (ART)	1104
3. Blurring Distinctions	1105
<i>B. Legal Landscape</i>	1106
1. Targeting Pregnant Individuals.....	1106
2. Legislation Post- <i>Dobbs</i>	1108
III. PENALIZING REPRODUCTIVE HEALTH & THE DATA ECOSYSTEM	1109
<i>A. Law Enforcement Access to Reproductive Health Data</i>	1110
1. Reports and Dragnets	1110
2. Impacts Across Reproductive Health and Support Networks	1114
<i>B. Citizen Access to Reproductive Health Data</i>	1117
<i>C. Third-Party Access and Discrimination</i>	1120
IV. PROTECTING REPRODUCTIVE HEALTH PRIVACY	1122
<i>A. Privacy Self-Management</i>	1123
1. The Difficulties of Privacy Self-Management	1123
2. Reproductive Health Privacy Self-Management Case Study	1125
<i>B. Company Privacy Management</i>	1130
<i>C. Regulating and Enforcing Privacy</i>	1134
1. Minimizing Reproductive Health Surveillance.....	1134
2. The American Data Privacy and Protection Act (ADPPA).....	1140
CONCLUSION	1143

REPRODUCTIVE HEALTH SURVEILLANCE

ANYA E.R. PRINCE*

Abstract: It is estimated that one in four women will undergo an abortion and that over a quarter of women will face pregnancy loss. Nevertheless, the general public often underestimates the true rates of both pregnancy termination and complication. One likely reason for this underestimation is that reproductive health is something many individuals keep private from their friends, family, and coworkers. Yet, this personal secrecy is directly at odds with corporate data practices and commercial data sharing. In reality, a vast data ecosystem collects and monetizes all aspects of reproductive health. This ecosystem took on a new dimension in 2022, when the U.S. Supreme Court decided *Dobbs v. Jackson Women's Health Organization*. Since then, *Dobbs* has brought the lack of reproductive health privacy into stark relief and highlighted how intimate health data can be leveraged to identify and prosecute those seeking abortions. Reproductive health surveillance is omnipresent, expansive, and extremely problematic. But privacy concerns should not be limited to only protecting information about abortions or to only protecting information from access by law enforcement. Reproductive health, from contraception and pregnancy to infertility and assisted reproduction to pregnancy loss and abortion, are inextricably intertwined, and thus greater privacy protection of all reproductive health information is needed. Immediate solutions focus on individual self-management and company good will: women are encouraged to delete their period tracking apps or to adopt burner phones, and companies are pressured to make changes to their data collection and retention practices. More is desperately needed. Only with radical, sweeping changes to data privacy can we hope to move from reproductive health surveillance to meaningful reproductive health privacy.

INTRODUCTION

Approximately ten to fifteen percent of confirmed pregnancies result in miscarriage or stillbirth.¹ Additionally, approximately twenty percent of preg-

* Professor, University of Iowa College of Law. I am indebted to many individuals for helpful comments and suggestions on this work. Thanks, in particular, to Greer Donley, Nicholas Terry, Alicia Solow-Niederman, Leah Fowler, Nicholson Price, Jennifer Oliva, and participants in the University of Iowa Faculty Workshop. Thank you to Seung Woo Ban, Caroline Wadman, and Kathleen Foley for research support.

¹ *Pregnancy Loss*, OFF. ON WOMEN'S HEALTH, <https://www.womenshealth.gov/pregnancy/youre-pregnant-now-what/pregnancy-loss> [<https://perma.cc/L25L-Q223>] (Feb. 22, 2021). Estimates are that as many as twenty-five percent of pregnancies end in miscarriage, but in many instances a pregnant individual might not yet know that they are pregnant at the time of miscarriage. *Id.*; Greer Donley &

nancies are terminated.² Overall, it is estimated that one in four women will undergo an abortion³ and that over a quarter of women will face pregnancy loss.⁴ Nevertheless, the general public often underestimates the true rates of pregnancy termination and complication.⁵ One likely reason for this underestimation is that reproductive health is something many individuals keep private from their friends, family, and coworkers.⁶ Perhaps they want to wait to disclose their pregnancy until after the first trimester when there is a lower risk of miscarriage.⁷ Perhaps they do not want to disclose a history of abortion or pregnancy loss because of social stigma.⁸ Perhaps they want to tell a close

Jill Wieber Lens, *Abortion, Pregnancy Loss, & Subjective Fetal Personhood*, 75 VAND. L. REV. 1649, 1668 (2022); Jonah Bardos et al., *A National Survey on Public Perceptions of Miscarriage*, 125 OBSTETRICS & GYNECOLOGY 1313, 1313 (2015) (stating that 15% to 20% of pregnancies result in miscarriage).

² Rachel K. Jones et al., *Long-Term Decline in US Abortions Reverses, Showing Rising Need for Abortion as Supreme Court Is Poised to Overturn Roe v. Wade*, GUTTMACHER INST. (June 15, 2022), <https://www.guttmacher.org/article/2022/06/long-term-decline-us-abortions-reverses-showing-rising-need-abortion-supreme-court> [<https://perma.cc/L267-G2YY>]. This estimate does not include self-managed abortion, so the numbers are likely higher. *See id.* In this study, “pregnancy” did not include pregnancies that resulted in miscarriage. *Id.* This 20% termination rate was calculated using data from 2020. *Id.* It is a slight increase from recent estimates, but the rate had stayed between 18% and 20% for the last ten years. *Id.* Rates are likely to shift post-*Dobbs v. Jackson Women’s Health Organization* as more individuals face barriers to access to abortion. *See id.*

³ Rachel K. Jones & Jenna Jerman, *Population Group Abortion Rates and Lifetime Incidence of Abortion: United States, 2008–2014*, 112 AM. J. PUB. HEALTH 1284, 1288 (2022). Relatedly, approximately 1% to 2% of pregnancies are ectopic, meaning that the fertilized egg implants somewhere other than the uterus, most often in the fallopian tube. Danielle M. Panelli, Catherine H. Phillips & Paula C. Brady, *Incidence, Diagnosis and Management of Tubal and Nontubal Ectopic Pregnancies: A Review*, FERTILITY RSCH. & PRAC., Oct. 15, 2015, at 1, 1. Ectopic pregnancies can be life-threatening to the pregnant individual and are managed with medication or surgery, similar to termination. *Id.* at 1, 8.

⁴ Donley & Lens, *supra* note 1, at 1668.

⁵ Bardos et al., *supra* note 1, at 1313, 1315 (finding that a majority of respondents to a survey estimated that miscarriages occur in less than 6% of pregnancies despite the fact that miscarriages occur in up to 20% of all pregnancies); Audrey Kearney et al., *KFF Health Tracking Poll: Views on and Knowledge About Abortion in Wake of Leaked Supreme Court Opinion*, KAISER FAM. FOUND. (June 9, 2022), <https://www.kff.org/womens-health-policy/poll-finding/kff-health-tracking-poll-views-knowledge-abortion-2022/> [<https://perma.cc/WND8-P3DS>] (finding that almost half of U.S. adults estimated that 10% of women have had an abortion despite the fact that the true number is estimated to be around 24%).

⁶ *See* Donley & Lens, *supra* note 1, at 1662 (highlighting the similarities regarding silence surrounding both pregnancy loss and abortion).

⁷ *Id.* at 1679.

⁸ Franz Hanschmidt et al., *Abortion Stigma: A Systematic Review*, 48 PERSPS. ON SEXUAL & REPROD. HEALTH 169, 175 (2016) (conducting a systematic review on abortion stigma and finding that the majority of included studies determined that those who had undergone abortion had a need for secrecy or were worried about social judgment); Jennifer J. Bute, Maria Brann & Rachel Hernandez, *Exploring Societal-Level Privacy Rules for Talking About Miscarriage*, 36 J. SOC. & PERS. RELATIONSHIPS 379, 380–81 (2019) (discussing literature reviewing the social stigma and misunderstandings around miscarriage that lead individuals to keep their history of pregnancy loss secret); Donley & Lens, *supra* note 1, at 1667–71 (discussing the stigma associated with both pregnancy

friend, but not publicly broadcast their health history.⁹ This understandable culture of secrecy means that many people fail to realize how common it is for individuals to face difficult reproductive health complications and decisions.

Yet, this personal secrecy is directly at odds with corporate data practices and commercial data sharing. Despite the relative shroud of secrecy cloaking many reproductive health decisions, copious amounts of sensitive information about reproduction is collected by companies and data brokers on a daily basis.¹⁰ Individuals who might not wish to announce the use of contraception or a miscarriage to a coworker may still disclose this information to a “Femtech” mobile app that tracks menstruation and fertility.¹¹ Those who are trying to conceive or those who are considering a pregnancy termination may not discuss this with family members, but may conduct web searches or purchase products online that clue in companies to intimate details about their reproductive health.¹² Indeed, to some, consulting resources on a cellphone in the confines of one’s home may feel more private than other means of gathering information and support.¹³ This, however, is far from true.

In reality, a vast data ecosystem distributes reproductive health information among companies and data brokers. Provocatively called “uterus surveillance,”¹⁴ “menstrual surveillance,”¹⁵ or “vaginal digitalization,”¹⁶ compa-

loss and abortion). *But see* Nina Cesare et al., *Discussions of Miscarriage and Preterm Births on Twitter*, 34 PAEDIATRIC & PERINATAL EPIDEMIOLOGY 544, 545 (2020) (highlighting that some individuals are quite public with their pregnancy loss and that this can increase when celebrities disclose their own experiences); Donley & Lens, *supra* note 1, at 1671 (noting various social media campaigns aimed at raising awareness and breaking the stigma of pregnancy loss and abortion).

⁹ Studies regarding misestimates of miscarriage and abortion rates often find that men are more likely to incorrectly estimate the true rates than women. Bardos et al., *supra* note 1, at 1315. This may indicate that women are more likely to be aware of the lived experiences of a broader range of their friends or family members. *See id.* (noting that “the odds of men reporting that miscarriages are uncommon was [greater than] that of women”); Kearney et al., *supra* note 5 (“Men are more likely than women to underestimate the share of women who have had an abortion . . .”).

¹⁰ Alfred Ng, *Data Brokers Resist Pressure to Stop Collecting Info on Pregnant People*, POLITICO (Aug. 1, 2022), <https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988> [<https://perma.cc/FNL4-A6DZ>]. Data brokers are “companies that specialize in the collection and exchange of personal information.” Matthew Crain, *The Limits of Transparency: Data Brokers and Commodification*, 20 NEW MEDIA & SOC’Y 88, 90 (2016).

¹¹ As will be discussed further below, “Femtech” is a term used to describe technology and mobile phone applications (“apps”) that relate to women’s reproductive health. Michele Estrin Gilman, *Periods for Profit and the Rise of Menstrual Surveillance*, 41 COLUM. J. GENDER & L. 100, 101 (2021).

¹² Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html> [<https://perma.cc/37V7-W4ES>].

¹³ Leah R. Fowler & Stephanie R. Morain, *Schrödinger’s App*, 46 AM. J.L. & MED. 203, 207 (2020) (discussing how some individuals feel that cellphone apps afford them more privacy than other methods of getting the same information).

¹⁴ Arwa Mahdawi, Opinion, *Will Anti-abortionists Use ‘Uterus Surveillance’ Against Women in the US?*, THE GUARDIAN (June 7, 2022), <https://www.theguardian.com/commentisfree/2022/jun/07/will-anti-abortionists-use-uterus-surveillance-against-women-in-the-us-roe-v-wade> [<https://perma.cc/>

nies generate a digital trail of information that is incredibly difficult to avoid.¹⁷ What's more, companies make billions of dollars off this personal data.¹⁸ Uterus surveillance, meet "surveillance capitalism."¹⁹

Reproductive health data comes not only from individuals directly sharing information with companies, but also from data brokers triangulating information to infer reproductive health status.²⁰ Thus, data about reproductive health can be both intentionally and unintentionally shared by women and those who can get pregnant.²¹ The information is valuable, in part, because it is of unique interest to advertisers. Pregnant individuals are particularly attractive to marketers because shopping habits will change both during pregnancy and after

5AVP-4E77]. Uterus surveillance is a subset of broader sexual privacy. For discussions of privacy-related issues regarding intimate life, from reproductive health to sexual preferences to dating habits, see generally Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019), and Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763 (2021) [hereinafter Citron, *A New Compact*].

¹⁵ Gilman, *supra* note 11, at 102.

¹⁶ Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?*, WASH. POST (Apr. 10, 2019) (quoting Natasha Felizi & Joana Varon, *Menstruapps – Como Transformar Sua Menstruação em Dinheiro (Para os Outros)?*, CHUPADADOS: CODING RTS., <https://chupadados.codingrights.org/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/> [<https://perma.cc/32U2-J2CB>]), <https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/> [<https://perma.cc/4TBG-25DG>].

¹⁷ See *infra* Section IV.A.

¹⁸ Gilman, *supra* note 11, at 101 (noting that "the booming Femtech industry is expected to be worth \$50 billion by 2025" (citing Donna Rosato, *What Your Period Tracker App Knows About You*, CONSUMER REPS., <https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you-a8701683935/> [<https://perma.cc/T5R9-VHUU>] (Jan. 28, 2020))).

¹⁹ "Surveillance capitalism" is a phenomenon where personal data is sold for profit by developing behavioral profiles of individuals that can be used in targeted advertising and algorithms. Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 75–76 (2015) (coining the phrase "surveillance capitalism"); SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* 8 (2019) ("Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data.").

²⁰ See *infra* Section I.A.

²¹ Some individuals who are pregnant or who menstruate identify as male or nonbinary rather than as female. Gilman, *supra* note 11, at 108. In this Article, the use of "female" or "woman" to describe any aspect of reproductive health privacy is not meant to be at the exclusion of those who identify differently. Reproductive health privacy is equally, if not much more, important to these individuals. Additionally, this Article focuses on the reproductive health of women and those who menstruate, although the data ecosystem of sharing medical information related to men's reproductive health, and indeed health information broadly, would be similar. The focus on women, however, is important because it is women's bodies that have been and continue to be under attack, excessively surveilled, and criminalized, making privacy of their information all the more essential.

birth.²² If a company is able to secure loyalty from pregnant individuals, it stands to capture significant profits.²³

Yet, companies and data brokers are not the only parties interested in gaining access to this treasure trove of data.²⁴ Following the U.S. Supreme Court's 2022 decision in *Dobbs v. Jackson Women's Health Organization*, the wide availability of reproductive health data is especially alarming.²⁵ Information about pregnancy outcomes can now increasingly lead to investigation and prosecution by police, and use by anti-abortion activists in states that have banned or restricted abortion.²⁶

Although the *Dobbs* ruling sets back reproductive rights fifty years, today's world is notably different in several key respects. Technological advances have altered key aspects of reproductive health, from enabling medication abortion outside of the clinic to assisting reproduction through in vitro fertilization (IVF).²⁷ These advances circumscribe traditional models of abortion care and challenge conceptions of when life begins—such transformations impact how new criminal laws are drafted, interpreted, and enforced. Before *Roe v. Wade*, laws criminalizing abortion predominately focused on providers.²⁸ But, in part because of increased access to medication abortion, anti-abortion laws and proposals increasingly target pregnant individuals themselves,²⁹ dras-

²² Duhigg, *supra* note 12 (reporting that “[i]f companies can identify pregnant shoppers, they can earn millions”).

²³ Gilman, *supra* note 11, at 104 (“[I]n the United States, a pregnant woman’s data is worth fifteen times that of the average person.” (citing *No Body’s Business but Mine: How Menstruation Apps Are Sharing Your Data*, PRIV. INT’L, <https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data> [<https://perma.cc/7L65-WFKY>] (Oct. 7, 2020))).

²⁴ In addition to the consequences associated with law enforcement access that are discussed in this paragraph, other negative outcomes—such as higher insurance costs and loan rates or lost job opportunities for pregnant women—can arise if employers, insurers, or lenders utilize reproductive health information. See *infra* Section III.C.

²⁵ See *Dobbs v. Jackson Women’s Health Org.*, 142 S. Ct. 2228, 2242 (2022) (overruling *Roe v. Wade*, 410 U.S. 113 (1973)).

²⁶ See generally ALBERT FOX CAHN & ELENI MANIS, PREGNANCY PANOPTICON: ABORTION SURVEILLANCE AFTER *ROE* (2022) (discussing potential digital surveillance of pregnant people in the post-*Dobbs* world). For the latest updates on frequent changes in state abortion laws, see *Interactive Map: US Abortion Policies and Access After Roe*, GUTTMACHER INST., <https://states.guttmacher.org/policies/> [<https://perma.cc/A6Y3-JVXQ>] (Apr. 24, 2023). Several excellent forthcoming articles grapple with various aspects of the privacy implications of the *Dobbs* decision. See generally Aziz Huq & Rebecca Wexler, *Digital Privacy for Reproductive Choice in the Post-Roe Era*, 97 N.Y.U. L. REV. (forthcoming 2023); Leah R. Fowler & Michael R. Ulrich, *Femtechnodystopia*, 75 STAN. L. REV. (forthcoming 2023); Wendy A. Bach & Nicholas Terry, *HIPAA v. Dobbs*, BERKELEY TECH. L.J. (forthcoming).

²⁷ See *infra* Section II.A.

²⁸ See *infra* Section II.B.

²⁹ David S. Cohen, Greer Donley & Rachel Rebouché, *Abortion Pills*, 76 STAN. L. REV. (forthcoming 2024) (manuscript at 27–29) (on file with author).

tically expanding the existent criminalization of pregnancy outcomes and behaviors.³⁰

Growing risks of criminalization will not be borne only by those seeking abortion care.³¹ Any woman who experiences a pregnancy loss could face suspicion. As states pass more extreme abortion restrictions, anyone pregnant could have their behaviors, such as use of medications, alcohol intake, or diet, questioned. Similarly, individuals seeking to grow their families through advanced reproductive technologies, like IVF, could find their actions scrutinized.³² If the Supreme Court continues to whittle away constitutional rights, even data about using contraceptives could become a liability.³³ Tragically, marginalized communities will likely continue to be disproportionately targeted by criminalization efforts, exacerbating existing societal disparities.³⁴

In a post-*Dobbs* world, threats of prosecution and civil liability collide with the robust reproductive health data ecosystem. Legal cases are, after all, built upon data.³⁵ And the data ecosystem is vastly different post-*Dobbs* than pre-*Roe*. Consequently, individuals who can get pregnant are vulnerable to surveillance and legal risk, especially those in marginalized communities.³⁶ But the potential negative harms of the data ecosystem go beyond use by law enforcement. Use of robust data sets by other entities, such as employers, lenders, and insurers, can also lead to disparate harms for those who can get pregnant.³⁷

In response to growing concerns about reproductive health privacy—or a lack thereof—individuals have been encouraged to delete period tracking apps,³⁸ download privacy-enhancing technology, and even get burner phones.³⁹

³⁰ *Id.*; *infra* Section II.B.

³¹ *See infra* Subsection III.A.2.

³² *See infra* Subsection II.B.2.

³³ Although the right to access contraception is currently protected, Justice Clarence Thomas called this right into question in his concurrence in *Dobbs*, writing that the Court “should reconsider all of this Court’s substantive due process precedents, including *Griswold*, *Lawrence*, and *Obergefell*.” *Dobbs v. Jackson Women’s Health Org.*, 142 S. Ct. 2228, 2301 (2022) (Thomas, J., concurring); *see also* Michael Ollove, *Some States Already Are Targeting Birth Control*, PEW (May 19, 2022), <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/05/19/some-states-already-are-targeting-birth-control> [<https://perma.cc/46RF-79AD>] (discussing state legislative efforts related to funding and minimizing access to contraception).

³⁴ MICHELE GOODWIN, *POLICING THE WOMB: INVISIBLE WOMEN AND THE CRIMINALIZATION OF MOTHERHOOD* 122–23 (2020).

³⁵ Huq & Wexler, *supra* note 26 (manuscript at 13) (noting that law enforcement relies upon the availability of information in abortion cases).

³⁶ *See infra* Subsection I.B.3.

³⁷ *See infra* Section III.C.

³⁸ Kendra Albert, Maggie Delano & Emma Weil, *Okay, Fine, Let’s Talk About Period Tracking: The Detailed Explainer*, MEDIUM (June 28, 2022), <https://medium.com/@maggied/okay-fine-lets-talk-about-period-tracking-the-detailed-explainer-2f45112eebb4> [<https://perma.cc/D6XP-TK2Y>].

Companies have been pressured to improve their data privacy practices, and healthcare providers have had to think carefully about how to protect patients' sensitive data.⁴⁰ Yet, if the current state of reproductive health privacy is a leaky boat, individual self-management and company efforts are simply buckets bailing out some of the water collecting in the hull. Although these efforts may minimize the volume of liquid amassing, ultimately, they will not fix the problem. Indeed, the leaky reproductive health data ecosystem is designed to maximize the leaking to contribute toward company profits.⁴¹ Thus, to move from reproductive health surveillance to truly meaningful reproductive health privacy, wholesale and fundamental changes to the data ecosystem are needed.

This Article proceeds in four parts. Part I maps the vast reproductive health data ecosystem and its associated harms, and then details how the current lack of federal data protections allows companies to amass intimate health data.⁴² Part II highlights key changes in both the medical and legal landscape that have taken place since the pre-*Roe* era.⁴³ Using two key examples, medication abortion and assisted reproductive technologies, Part II shows how advances in reproductive care increase healthcare options for individuals, but also leave data trails associated with sensitive reproductive choices. It discusses why this data trail and the underlying reproductive health data ecosystem are so problematic given the likelihood of increased criminalization and investigation of pregnancy and pregnancy outcomes. These harms will not only impact those seeking abortion care, but also affect individuals across a broad range of reproductive health conditions, from those experiencing pregnancy loss to those who are pregnant, to, possibly, those taking contraceptives or seeking infertility treatments. As Part III confirms, law enforcement, everyday citizens, employers, and insurers can access wide-scale data about reproductive health, increasing risks of prosecution, civil liability, and discrimination for those who can get pregnant.⁴⁴ Given these troubling harms, Part IV examines possible solutions, including privacy self-management, changing company practices, and congressional legislation.⁴⁵ Individual and company efforts are band-aids at best—important, but unlikely to truly make a dent in the problem.

³⁹ Daly Barnett, *Security and Privacy Tips for People Seeking an Abortion*, ELEC. FRONTIER FOUND. (June 23, 2022), <https://www.eff.org/deeplinks/2022/06/security-and-privacy-tips-people-seeking-abortion> [<https://perma.cc/FJ4Q-KVFN>].

⁴⁰ See Kayte Spector-Bagdady & Michelle M. Mello, *Protecting the Privacy of Reproductive Health Information After the Fall of Roe v. Wade*, JAMA HEALTH F., June 2022, at 1, 2, <https://jamanetwork.com/journals/jama-health-forum/fullarticle/2794032> [<https://perma.cc/H2QY-2BNL>].

⁴¹ See *infra* Section I.B.

⁴² See *infra* Part I.

⁴³ See *infra* Part II.

⁴⁴ See *infra* Part III.

⁴⁵ See *infra* Part IV.

Instead, wholesale, radical realignment of our country's data privacy framework is needed. Several bills in Congress aim to do just that. This Article argues that four key aspects of reproductive health privacy regulation are sorely needed: (1) regulation of data brokers and the data ecosystem fueled by monetization; (2) regulation of reproductive health information, both direct and inferred; (3) regulation of data collection itself; and (4) regulation across the states. Capturing these requirements in comprehensive and passable legislation is difficult. Yet, it is only with widescale, radical changes to our privacy landscape that we can hope to move our country from a system of reproductive surveillance to one promising meaningful reproductive health privacy.

I. THE REPRODUCTIVE HEALTH DATA ECOSYSTEM

Whether wittingly or unwittingly, individuals share vast amounts of information about reproductive health with private companies on a daily basis.⁴⁶ This Part explores this thorny problem. From internet searches regarding birth control to GPS location data pinpointing a cellphone at an abortion clinic, companies constantly amass private health information about millions of individuals. In an era of big data and data brokers, disparate information can be aggregated to paint an in-depth portrait of an individual's reproductive health.⁴⁷ This Part then discusses how companies have a strong profit incentive to collect such data and use it for targeted advertising, even when such use can lead to tangible harms.⁴⁸

The fact that someone is pregnant, trying to get pregnant, trying to avoid pregnancy, or had a miscarriage or an abortion is sensitive reproductive health information. And, as this Part discusses, although these facts would be relatively protected within a healthcare setting, they are at a greater risk of unwanted sharing in other realms.⁴⁹ This is because current federal U.S. privacy law is

⁴⁶ See *infra* Section I.A.

⁴⁷ See generally Paul Ohm & Scott Peppet, *What if Everything Reveals Everything?* (musing about the possibility that, with sufficient data aggregation, everything about a person can be discovered), in *BIG DATA IS NOT A MONOLITH* 45 (Cassidy R. Sugimoto, Hamid R. Ekbia & Michael Mattioli eds., 2016); Mason Marks, *Emergent Medical Data: Health Information Inferred by Artificial Intelligence*, 11 U.C. IRVINE L. REV. 995, 1000–13 (2021) (highlighting how data aggregation can illuminate a person's health conditions); Anya E.R. Prince, *Location as Health*, 21 HOUS. J. HEALTH L. & POL'Y 43, 55–57 (2021) (discussing the specific example of how GPS location data can be used to infer health status, including use of abortion services).

⁴⁸ See *infra* Section I.B.

⁴⁹ This Part discusses ways that individuals share reproductive health information with companies, both directly and knowingly and indirectly and perhaps unknowingly. There are other ways that companies could get specific information about an individual's pregnancy, such as through shadow medical records. See W. Nicholson Price II, Margot E. Kaminski, Timo Minssen & Kayte Spector-Bagdady, *Shadow Health Records Meet New Data Privacy Laws*, 363 SCIENCE 448, 448 (2019)

siloed—it revolves, not only around the type of data at issue, but also around who holds this data.⁵⁰ If a doctor has information that a patient is pregnant, this information is protected under federal privacy law.⁵¹ The same cannot be said if a mobile app developer holds the same information.⁵²

A. Reproductive Health Information Sharing

Although many people view their reproductive health data as intimate and private, this information is, in reality, broadly collected and regularly shared by companies.⁵³ In many cases, individuals directly share information about reproductive health with companies.⁵⁴ In other cases, individuals may, perhaps unintentionally, share information that can be used to infer private reproductive health status.⁵⁵

1. Direct Information Sharing

Many individuals directly provide companies with information about their reproductive health, such as their use of birth control, fertility treatments, pregnancy, pregnancy loss, or termination. For example, a woman may post on social media that she is pregnant or may join an online support group for women who have faced pregnancy loss. These public-facing actions give companies and—depending on user privacy settings—the broader public, information about reproductive health.⁵⁶ Companies, however, often collect and use this data even when individuals use “private” settings on social media where only certain users—perhaps in a “private” social media group—can see a post or comment.⁵⁷

(highlighting the existence of shadow medical records that sit outside of the protections of health privacy laws but cover the same information as that within the healthcare system).

⁵⁰ See *infra* Section I.C.

⁵¹ See *infra* Section I.C.

⁵² See *infra* Section I.C.

⁵³ This Section focuses on the flow of information between individuals and companies, generally without any intermediary. It is important to note, however, that individuals often share information with friends and families in ways that could increase access by companies. For example, many apps discussed in this Section allow users to share accounts with intimate partners or friends in ways that create information vulnerabilities. See, e.g., Leah R. Fowler, Charlotte Gillard & Stephanie Morain, *Teenage Use of Smartphone Applications for Menstrual Cycle Tracking*, PEDIATRICS, May 2020, at 1, 2 (highlighting that, in pediatric populations, period app information is often shared with partners, parents, and friend groups).

⁵⁴ See *infra* Subsection I.A.1.

⁵⁵ See *infra* Subsection I.A.2.

⁵⁶ See, e.g., Cesare et al., *supra* note 8, at 546–48 (researching public Twitter posts regarding miscarriage and preterm births).

⁵⁷ See, e.g., Kirsten Osther & Fred Trotter, *Facebook’s FTC Settlement Doesn’t Protect Privacy of Users’ Health Information*, STAT (July 31, 2019), <https://www.statnews.com/2019/07/31/facebook->

One of the largest sources of direct data sharing between individuals and companies regarding reproductive health is the so-called “Femtech” industry.⁵⁸ Femtech refers to technology that is meant to assist individuals, particularly women, with tracking and managing their reproductive health.⁵⁹ Although the Femtech industry is steeped in the “rhetoric of feminist empowerment,” it transforms women en masse into valuable data points.⁶⁰ Nearly one third of U.S. women and over one hundred million women around the globe interact with Femtech apps.⁶¹ By 2025, the industry is expected to have a fifty billion dollar valuation.⁶²

There are numerous ways within these apps that companies learn about individuals’ reproductive health. For example, users track their periods using an application interface, thus providing specific details about pregnancies, birth, and loss or termination of pregnancies. App users may also be asked to report intimate details about their sex lives, pregnancy and abortion history, and other aspects of reproductive health.⁶³ Some users may opt to post additional details on discussion boards tracked by the companies.⁶⁴ After one becomes pregnant, other apps track pregnancies by week, informing individuals of the size of their fetus or the latest developments *in utero*.⁶⁵

ftc-settlement-health-information-privacy/ [https://perma.cc/JWR9-5B9Q] (highlighting complaints made to the Federal Trade Commission (FTC) alleging that Facebook (now Meta) encouraged individuals to join “private” health-related support groups and then collected and sold the resulting health data to third parties).

⁵⁸ Michele Estrin Gilman, *Feminism, Privacy, and Law in Cyberspace* (noting that the term “Femtech” originated with Ida Tin, the CEO of a period-tracking app), in *THE OXFORD HANDBOOK OF FEMINISM AND LAW IN THE UNITED STATES* § III.C (Deborah Brake, Martha Chamallas & Verna L. Williams eds., 2021). See generally Fowler & Ulrich, *supra* note 26 (discussing the Femtech industry and the implications of the *Dobbs* decision).

⁵⁹ Gilman, *supra* note 11, at 101.

⁶⁰ See Gilman, *supra* note 58, § III.C.

⁶¹ Citron, *A New Compact*, *supra* note 14, at 1775; Fowler & Morain, *supra* note 13, at 206.

⁶² Gilman, *supra* note 11, at 101. This valuation is all the more impressive when one realizes that many of the Femtech apps that track menstrual cycles are free to users. *Id.* at 113. The profits stem from selling valuable reproductive health information to advertisers and other third parties that are willing to pay. *Id.* at 102–03; see also Harwell, *supra* note 16 (discussing how lucrative women’s bodies are).

⁶³ See, e.g., Harwell, *supra* note 16 (noting that one Femtech app asks users to report on the results of a pregnancy, including pregnancy loss). Some of the data collected can get very specific and detailed, such as physical aspects of menstrual flow or cervical mucus. E.g., Gilman, *supra* note 11, at 103.

⁶⁴ Citron, *A New Compact*, *supra* note 14, at 1776 (noting how Femtech apps track discussion board communications).

⁶⁵ See Deborah Lupton & Gareth M. Thomas, *Playing Pregnancy: The Ludification and Gamification of Expectant Motherhood in Smartphone Apps*, *MEDIA/CULTURE J.* (2015), <https://journal.media-culture.org.au/index.php/mcjournal/article/view/1012> [https://perma.cc/WZ9G-XU4D] (highlighting that popular pregnancy tracking apps have been downloaded millions of times).

Often, an individual chooses to disclose reproductive health data to companies precisely because they need some pertinent information or service in return. For example, if an individual needs to take a Lyft rideshare to an abortion provider, they may put the address into the app, thus cluing in the company about their visit to a clinic.⁶⁶ Similarly, individuals may have no place to begin when they have reproductive health-related questions, other than to conduct internet searches for answers or to connect with social media support networks.⁶⁷ For others, online platforms, such as Facebook Messenger, may be a key method of communication with friends and family.⁶⁸ Thus, disclosing reproductive health information to companies can be necessary to gain access to needed information, resources, or support groups.

Sometimes, when individuals directly share information about reproductive health, they do so openly without any expectations of privacy, such as by publicly posting on Twitter about their history of pregnancy loss. But in many instances, individuals directly sharing sensitive information with companies may believe the information is more protected than it actually is.⁶⁹ As will be discussed, the shared data may not have much protection at all, and are likely to be sold or shared freely without much customer control.⁷⁰

⁶⁶ Of course, the individual could put in an address of a place near the clinic rather than the clinic itself, but to find this information one would likely need to look at a map to see what the nearby addresses are, thus putting the address into Apple or Google maps and sharing this information anyway.

⁶⁷ It is important to note that just because individuals utilize online resources for answers to these medical questions, it does not mean that they will receive accurate information. See, e.g., Fowler & Morain, *supra* note 13, at 206–07 (noting that Femtech apps are rife with accuracy problems, which could lead to many women miscalculating their ovulation windows—a big problem for both those trying to conceive and those trying to avoid pregnancy); see also Citron, *A New Compact*, *supra* note 14, at 1777 (citing research finding that over 80% of free Femtech apps assessed were “inaccurate, contain[ed] misleading health information, or d[id] not function” (alterations in original) (quoting Jerry Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats*, *Consumer Reports Finds*, CONSUMER REPS., <https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats-a1100919965/> [<https://perma.cc/A4VM-9GPA>] (Sept. 17, 2020))).

⁶⁸ Cf. Martin Kaste, *Nebraska Cops Used Facebook Messages to Investigate an Alleged Illegal Abortion*, NPR (Aug. 12, 2022), <https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion> [<https://perma.cc/MM7N-E93N>] (detailing how a police department utilized private Facebook messages between a woman and her teenage daughter to investigate an alleged illegal abortion).

⁶⁹ See, e.g., Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1886 (2013); see also Leah R. Fowler, Charlotte Gillard & Stephanie R. Morain, *Readability and Accessibility of Terms of Service and Privacy Policies for Menstruation-Tracking Smartphone Applications*, 21 HEALTH PROMOTION PRAC. 679, 681 (2020) (studying the readability of privacy policies for Femtech apps and finding that “it is likely that many users do not comprehend how their data are used and shared”).

⁷⁰ See *infra* Section I.C.

2. Indirect Information Sharing

In addition to direct information sharing, companies constantly collect individual data that can be used to infer private reproductive health information.⁷¹ A simple example of this is the collection of GPS location data.⁷² GPS location data are ubiquitously collected by cellphone companies and associated applications.⁷³ The data make it easy to discover that a woman has been regularly going to an IVF clinic or has visited an abortion clinic, and thereby allow companies to infer her reproductive health status.⁷⁴ Indeed, advertisers have specifically utilized location data to make such inferences. In a notable case, an advertising firm created a “geofence” around abortion clinics.⁷⁵ Individuals who entered the virtual “fenced” location were sent adver-

⁷¹ The growing ability of companies to infer information about individuals with enough data is well-discussed in the literature. See, e.g., Prince, *supra* note 47, at 77–78 (highlighting how the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936, does not protect health data that can be inferred from location information); Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257, 1283 (2020) (discussing a related problem of how the ability to link neutral data to protected information increases the risk of discrimination); Solon Barocas & Helen Nissenbaum, *Big Data’s End Run Around Anonymity and Consent*, in *PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT* 44, 55–56 (Julia Lane, Victoria Stodden, Stefan Bender & Helen Nissenbaum eds., 2014); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96 (2014); Marks, *supra* note 47, at 1000–13 (discussing “emergent medical data” that can be inferred from innocuous data points); Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 361 (2022) (discussing how inferences challenge existing privacy frameworks); Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL’Y L. & ETHICS 143, 147 (2017) (highlighting the problem of “medically inflected” data).

⁷² See generally Prince, *supra* note 47, at 52–57, 65 (highlighting the various ways that GPS location data can be used to infer health information, including reproductive health information).

⁷³ Stuart A. Thompson & Charlie Warzel, Opinion, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html> [<https://perma.cc/PME2-HL32>].

⁷⁴ See, e.g., Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022), <https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood> [<https://perma.cc/8S93-HMLR>] (noting that one could obtain data regarding what phones entered a Planned Parenthood clinic over the course of a week for the low cost of \$160). Of course, these inferences will not always be correct. Prince, *supra* note 47, at 56 (noting that location data showing an individual at a Planned Parenthood site allow an inference that the individual is having an abortion, even though the person could instead be driving a friend to an appointment, getting a well-woman visit, volunteering, or even protesting against abortion); see also Gilman, *supra* note 11, at 104 n.20 (noting the inaccuracies of reports from data brokers (citing Caitlyn Renee Miller, *I Bought a Report on Everything That’s Known About Me Online*, THE ATLANTIC (June 6, 2017), <https://www.theatlantic.com/technology/archive/2017/06/online-data-brokers/529281/> [<https://perma.cc/732V-8WNU>])); Miller, *supra* (reporting that approximately half of the information that a data broker provided about the author was incorrect).

⁷⁵ Press Release, Off. of Mass. Att’y Gen., AG Reaches Settlement with Advertising Company Prohibiting ‘Geofencing’ Around Massachusetts Healthcare Facilities (Apr. 4, 2017), <https://www.>

tisements that focused on alternatives to abortion and would continue to receive these anti-choice advertisements for the next thirty days.⁷⁶

Beyond GPS location data, a dizzying array of information can be used to infer reproductive health status, from product purchases,⁷⁷ to internet searches, to changes in food or alcohol consumption. Nearly every aspect of our lives is now under digital surveillance. Smart refrigerators may help you create a grocery list, but they could also send data about food consumption to companies.⁷⁸ A website may help provide answers to questions about early signs of pregnancy or how to obtain abortion medication, but data from electronic trackers monitoring traffic to the website may also be stored far into the future.

In an era of big data and artificial intelligence, companies have the power to make inferences about individuals' health from a wide variety of data points.⁷⁹ The more data points a company has from an individual, the more accurate and reliable the predictions can be.⁸⁰ To complicate matters further, this indirect piecing together of health information can be aggregated by a third party after collecting many innocuous pieces of information from different sources.⁸¹ This makes it incredibly difficult for an individual to assess whether any one company has too much information about them. They may feel comfortable sharing location data with Company A, providing information to Company B through purchase history that they are no longer drinking alcohol, and showing Company C that they are searching for the meanings of various names, not realizing that

mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities [https://perma.cc/E8DF-WGFJ].

⁷⁶ Citron, *A New Compact*, *supra* note 14, at 1808–09 (noting that the Massachusetts Attorney General's Office argued that these were “unfair and deceptive business practices”). The case settled. Press Release, *supra* note 75.

⁷⁷ Duhigg, *supra* note 12 (raising the example of Target identifying pregnant shoppers through seemingly innocuous purchases).

⁷⁸ Renée Lynn Midrack, *What Is a Smart Refrigerator?*, LIFEWIRE, <https://www.lifewire.com/smart-refrigerator-4158327> [https://perma.cc/Q58B-LD7F] (July 24, 2021); Roberto Yus & Primal Pappachan, *Smart Devices Spy on You—2 Computer Scientists Explain How the Internet of Things Can Violate Your Privacy*, THE CONVERSATION (Mar. 14, 2022), <https://theconversation.com/smart-devices-spy-on-you-2-computer-scientists-explain-how-the-internet-of-things-can-violate-your-privacy-174579> [https://perma.cc/WMQ2-B5WX]; Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1372–73 (2017).

⁷⁹ Mason Marks, *Tech Companies' Dangerous Practice: Using Artificial Intelligence to Mine Hidden Health Data*, STAT (Sept. 17, 2019), <https://www.statnews.com/2019/09/17/digital-traces-tech-companies-artificial-intelligence/> [https://perma.cc/FG5U-CP9J] (“Tech companies feed our digital traces into machine learning algorithms and, like modern day alchemists turning lead into gold, transform seemingly mundane information into sensitive and valuable health data.”); *see also* Marks, *supra* note 47, at 1000–02.

⁸⁰ *See* Ohm & Peppet, *supra* note 47, at 50.

⁸¹ Solove, *supra* note 69, at 1889–93.

all three companies are selling consumer data to Company D, which allows Company D to infer that the individual is likely pregnant.⁸²

B. Monetizing the Reproductive Health Data Ecosystem

Companies are motivated to amass as much information about consumers as possible because data have become “the coin of the realm.”⁸³ This commodification of individuals’ data has spawned vast markets trading in valuable personal information where companies sell collected consumer information to third parties, such as data brokers,⁸⁴ data analytics firms,⁸⁵ or advertisers.⁸⁶ These companies may share the data even further.⁸⁷ Beyond companies that specialize in aggregating data, other entities, such as employers or insurance companies, can purchase data.⁸⁸ Theoretically, almost anyone could purchase data about individuals, often for fairly low costs.⁸⁹ Sometimes, the information

⁸² See FED. TRADE COMM’N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 47 (2014) (reporting that data brokers use inferences to categorize customers as, among other things, “[e]xpectant [p]arent[s]”).

⁸³ Citron, *A New Compact*, *supra* note 14, at 1767; *The World’s Most Valuable Resource Is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> [<https://perma.cc/DGS8-L493>].

⁸⁴ Crain, *supra* note 10, at 90 (“The business of data brokers can be classified into two basic processes of data acquisition and data monetization.”). A well-known example of a data broker is Experian, one of the companies that gathers the credit scores of individuals. Christopher K. Odinet, *Consumer Bitcredit and Fintech Lending*, 69 ALA. L. REV. 781, 787 & n.25 (2018).

⁸⁵ Data analytics firms assist companies in analyzing the data collected from individuals. See Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html> [<https://perma.cc/AA5T-KQG8>]. An infamous data analytics company is Cambridge Analytica, which became well-known in 2018 for accessing millions of Facebook users’ information and using this data to influence voting behaviors. *Id.*

⁸⁶ Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FED. TRADE COMM’N: BUS. BLOG (July 11, 2022), <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal> [<https://perma.cc/Q3F7-V6SM>] (noting that consumer data often ends up in the hands of marketers).

⁸⁷ See Elvy, *supra* note 78, at 1372.

⁸⁸ The selling, buying, and aggregating of data among companies, insurers, and employers is all anticipated and intentional data sharing. Data sharing can, of course, also happen unintentionally if there are lax security protections on user data that allow hackers to access private data. See, e.g., Citron, *A New Compact*, *supra* note 14, at 1769 (highlighting how hackers may be particularly interested in information revealing intimate details about individuals). For example, a Consumer Reports study on Femtech apps revealed serious vulnerabilities in an app created by Glow, Inc. See Beilinson, *supra* note 67. Due to poor design, intimate user information could have been identified by anyone who knew the user’s email address. *Id.* The California Attorney General settled with the company to fix the vulnerabilities. *Id.* Additionally, data may be accessible to law enforcement through warrants—a concern that will be discussed further below. See *infra* Section III.A.

⁸⁹ For example, location data has been sold for costs as low as a couple hundred dollars. See Joseph Cox, *FCC to Propose Fines of AT&T, T-Mobile, Sprint, Verizon for Selling Location Data*, VICE

is sold in de-identified, aggregate form, so that it is not directly linked to any one individual. But research indicates that de-identified information can often easily be re-identified.⁹⁰

This broad sharing of personal data has both upsides and downsides. Many of the conveniences that we enjoy daily through free apps or resources on the web are made possible because of the commodification of data. There are, however, harms to this ecosystem as well, especially when it comes to reproductive health information. This Section discusses the harms of targeted advertising,⁹¹ the broader harms of the reproductive data ecosystem,⁹² and the disparate impacts of these harms.⁹³

1. Targeted Advertising and Harms

One key result of the commodification of personal data is that many technologies are available to users for free⁹⁴—at least in the monetary sense.⁹⁵ Consumers are paying for these technologies in the currency of data—that is, the user gets free access to a service in exchange for private information that can be sold or analyzed to create advertising profiles.⁹⁶ Indeed, many commentators flip the narrative and argue that when something is free, the customer is not a customer at all, but rather the product.⁹⁷

(Feb. 27, 2020), <https://www.vice.com/en/article/3a87bv/fcc-propose-fines-verizon-att-sprint-tmobile-selling-location-data> [<https://perma.cc/LED8-QLVS>]; see also Brian Barrett, *A Location-Sharing Disaster Shows How Exposed You Really Are*, WIRED (May 19, 2018), <https://www.wired.com/story/locationsmart-securus-location-data-privacy/> [<https://perma.cc/MA9Y-KH4S>] (“[A]ll four major US carriers sell location data to companies you’ve never heard of, without your explicit permission.”). More recently, a data broker stopped its practice of selling location data related to visits to Planned Parenthood locations. Hannah Norman & Victoria Knight, *Should You Worry About Data from Your Period-Tracking App Being Used Against You?*, KAISER HEALTH NEWS (May 13, 2022), <https://khn.org/news/article/period-tracking-apps-data-privacy/> [<https://perma.cc/YN4S-AB7L>]; see also *infra* Section III.C.

⁹⁰ See, e.g., Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1716–22 (2010) (highlighting how efforts at anonymizing data often fail); Stacey A. Tovino, *Not So Private*, 71 DUKE L.J. 985, 992–1006 (2022) (discussing the rampant risks of re-identification and analyzing de-identification standards across a variety of laws). The FTC recently indicated that it will increasingly scrutinize claims of anonymization given the potential for false promises; it remains to be seen what will come of this focus. See Cohen, *supra* note 86.

⁹¹ See *infra* Subsection I.B.1.

⁹² See *infra* Subsection I.B.2.

⁹³ See *infra* Subsection I.B.3.

⁹⁴ See, e.g., Elvy, *supra* note 78, at 1384–87 (describing traditional data models as free or “data-as-payment”).

⁹⁵ See generally John M. Newman, *The Myth of Free*, 86 GEO. WASH. L. REV. 513 (2018) (debunking the myth that “free” products are beneficial and actually free to individuals).

⁹⁶ Elvy, *supra* note 78, at 1384 (labelling this kind of compensation as “data-as-payment”).

⁹⁷ Olivia Solon, *You Are Facebook’s Product, Not Customer*, WIRED (Sept. 21, 2011), <https://www.wired.co.uk/article/doug-rushkoff-hello-etsy> [<https://perma.cc/GAF6-QR6Y>]; Karl Hodge, *If*

A primary consequence of the commodification of personal data is the flourishing of targeted advertising. Targeted advertising occurs when individuals are profiled into groups related to behaviors, interests, or other characteristics and then shown advertisements specifically designed to be of interest.⁹⁸ The use of cookies and identifiers across devices means that data and advertisements can follow a person across multiple devices.⁹⁹ Most everyone has likely had the somewhat jarring experience where they search for something on a computer—say beach vacation—and soon begin seeing advertisements for sunglasses and swimsuits on their phone or tablet. Although targeted ads may arise from a host of inferences about an individual, companies use health information to create targeted ads for medications, vitamins, or other goods related to the condition.¹⁰⁰ Marketers are especially interested in sending targeted advertisements to pregnant individuals given their expected purchasing habits during pregnancy and after birth.¹⁰¹

Some may view targeted advertising as helpful or, at the very least, innocuous. Indeed, some research shows that individuals are willing to trade their privacy for cheaper goods or other benefits, indicating that the public may find this trade-off beneficial in some circumstances.¹⁰² Additionally, the wide availability of “free” services may allow individuals to access and utilize important resources in ways they could not if companies had to make profits in some other way.¹⁰³

Nevertheless, targeted advertising carries negative consequences, especially in the context of reproductive health. A poignant example is the phe-

It's Free Online, You Are the Product, THE CONVERSATION (Apr. 19, 2018), <https://theconversation.com/if-its-free-online-you-are-the-product-95182> [<https://perma.cc/PN36-H8KL>].

⁹⁸ See, e.g., Prince, *supra* note 47, at 63–64 (discussing multiple ways that individuals' location data can be used to develop advertising of potentially greater interest to the individual). See generally FED. TRADE COMM'N, CROSS-DEVICE TRACKING (2017) (reporting on the use of “cross-device tracking,” which involves collecting information from multiple sources to learn about a consumer, often for targeted advertising).

⁹⁹ For a discussion regarding how advertisers can follow an individual across devices, see generally FED. TRADE COMM'N, *supra* note 98.

¹⁰⁰ See, e.g., Marks, *supra* note 47, at 1028–29 (noting that advertisers target ads based on health conditions and discussing some of the potential negative consequences of these ad campaigns).

¹⁰¹ Duhigg, *supra* note 12.

¹⁰² See Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 6–11 (2021) (summarizing the numerous studies that show that people's behaviors regarding privacy do not match their stated values of privacy in that, behaviorally, they are more willing to give up privacy in exchange for a benefit despite saying that they value privacy). It is important to note, however, that Professor Solove himself does not see a conflict between these behaviors and stated values because “[a]ttitudes are more general views about value and can exist beyond specific contexts. The fact that attitudes and behavior about privacy diverge is not a paradox or even an inconsistency.” *Id.* at 4.

¹⁰³ See Elvy, *supra* note 78, at 1387–92 (discussing revenue models that companies use to make money if they are not selling user data for profit).

nomenon of women continuing to receive pregnancy-related advertisements after experiencing a pregnancy loss.¹⁰⁴ Being bombarded with ads anticipating a happy family and smiling baby after experiencing loss can be extremely traumatizing and emotionally harmful.¹⁰⁵ Beyond potential emotional harm, targeted advertisements can also be weaponized to impact reproductive care. For example, as discussed above, targeted advertisements have been used by anti-abortion groups in an attempt to interfere with an individual's private reproductive medical choices.¹⁰⁶ Thus, targeted advertising to pregnant individuals has the potential for real and direct harm.

2. Other Harms

The reproductive health data ecosystem has several other potential harms worth noting. First, widespread data sharing leads to loss of individual control. As will be discussed, the U.S. privacy framework aspires to give individuals the choice of when and with whom to share private information.¹⁰⁷ In practice, however, this promise is illusory.¹⁰⁸ "Private-sector surveillance of intimate information strips individuals of the ability to decide who learns about their miscarriages, breakups, HIV infections, and sexual assaults, now and long into the future."¹⁰⁹ Data sharing, aggregation, and inferences lead to further difficulties in controlling what information is disclosed.¹¹⁰

¹⁰⁴ See, e.g., Rachael Louise Healy, *Zuckerberg, Get Out of My Uterus! An Examination of Fertility Apps, Data-Sharing and Remaking the Female Body as a Digitalized Reproductive Subject*, 30 J. GENDER STUD. 406, 411 (2021) (noting that Femtech apps and the targeted advertisements they generate sometimes fail to "recognize the crucial fact that getting pregnant does not always result in having a healthy baby, or even a baby at all," and that "[f]or the women mentioned above, and many others, the same fertility apps which claim to empower women have in fact played an active role in causing distress, trauma in these timely and misjudged markers"); see also Gilman, *supra* note 11, at 104 (explaining how "for women who have lost pregnancies . . . targeted profiling can be psychologically painful").

¹⁰⁵ I have written about my personal experiences with this trauma. Anya E.R. Prince, *I Tried to Keep My Pregnancy Secret*, THE ATLANTIC (Oct. 10, 2022), <https://www.theatlantic.com/ideas/archive/2022/10/can-you-hide-your-pregnancy-era-big-data/671692/> [<https://perma.cc/48RV-GG4X>]. I am not alone in this experience. See, e.g., Gillian Brockell, *Dear Tech Companies, I Don't Want to See Pregnancy Ads After My Child Was Stillborn*, WASH. POST (Dec. 12, 2018), <https://www.washingtonpost.com/lifestyle/2018/12/12/dear-tech-companies-i-dont-want-see-pregnancy-ads-after-my-child-was-stillborn/> [<https://perma.cc/2SPM-796X>]; Bridget de Maine, *After My Miscarriage, 'Big Data' Kept Haunting Me*, SYDNEY MORNING HERALD (June 19, 2019), <https://www.smh.com.au/lifestyle/life-and-relationships/reams-of-data-are-gathered-about-us-during-our-most-private-moments-20190618-p51z1d.html> [<https://perma.cc/9799-RYZM>].

¹⁰⁶ See *supra* Subsection I.A.2; see also Citron, *A New Compact*, *supra* note 14, at 1808–09.

¹⁰⁷ See *infra* Section I.C.

¹⁰⁸ See *infra* Section IV.A.

¹⁰⁹ Citron, *A New Compact*, *supra* note 14, at 1769.

¹¹⁰ Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 518–20 (2006).

When individuals feel a loss of control over their information, by learning that their private reproductive health information is so widely collected and sold, it may chill their behavior.¹¹¹ Individuals may avoid searching for important health data online, decide not to join an online group that could provide them with needed mental health support, or otherwise alter their behaviors in ways that are not beneficial to society.¹¹² As will be discussed, this worry over chilling behavior is especially relevant in the wake of *Dobbs*, as many lay media sources are encouraging women to ditch their fertility tracking apps and watch their online presence regarding abortion searches.¹¹³

Second, the commodification of reproductive health information affects society by threatening societal values and perpetuating harmful stereotypes and gendered norms.¹¹⁴ For example, the designs of Femtech apps are often deeply rooted in social stereotypes. One app sent messages to individuals who were trying to conceive and likely in their ovulation window encouraging them “to wear nice underwear” while also “sending notices to their partners to bring home flowers.”¹¹⁵ In these ways, data surveillance can threaten important values such as “self-expression[,] dignity[,] intimacy[,] and equality.”¹¹⁶

3. Inequitable Impacts

As is the unfortunate case in so many contexts, these potential harms are unlikely to fall equally across society. Marginalized communities are more likely to feel the harmful effects of the lack of reproductive privacy because they are more likely to be targeted by surveillance and face stigma or discrimination for reproductive choices.¹¹⁷ Indeed, there are already too many examples of minority women being surveilled and punished for reproductive choic-

¹¹¹ Cf. *id.* at 487 (describing the chilling effect in the context of police surveillance).

¹¹² See, e.g., Citron, *A New Compact*, *supra* note 14, at 1794.

¹¹³ See *infra* Part IV.

¹¹⁴ See, e.g., Healy, *supra* note 104, at 414 (discussing how Femtech apps are “playing a role in further medicalizing and dominating a social control over the female body as a reproductive machine”).

¹¹⁵ Gilman, *supra* note 58, § III.C (citing Kaitlyn Tiffany, *Period-Tracking Apps Are Not for Women*, VOX, <https://www.vox.com/the-goods/2018/11/13/18079458/menstrual-tracking-surveillance-glow-clue-apple-health> [<https://perma.cc/G6TR-VZYM>] (Nov. 16, 2018) (“Feminists value privacy for its autonomy-enhancing capacity. Femtech promises autonomy but often delivers the opposite.”)).

¹¹⁶ Citron, *A New Compact*, *supra* note 14, at 1792–93.

¹¹⁷ Lynn M. Paltrow & Jeanne Flavin, *Arrests of and Forced Interventions on Pregnant Women in the United States, 1973–2005: Implications for Women’s Legal Status and Public Health*, 38 J. HEALTH POL. POL’Y & L. 299, 311–12 (2013); Lynn M. Paltrow, *Pregnant Drug Users, Fetal Persons, and the Threat to Roe v. Wade*, 62 ALB. L. REV. 999, 1025 (1999); DOROTHY ROBERTS, *KILLING THE BLACK BODY: RACE, REPRODUCTION, AND THE MEANING OF LIBERTY* 159 (1997); Yvonne Lindgren, *The Doctor Requirement: Griswold, Privacy, and At-Home Reproductive Care*, 32 CONST. COMMENT. 341, 375 (2017).

es.¹¹⁸ For example, one study that examined criminalization of reproductive outcomes between 1973 and 2005 found that 59% of cases were brought against women of color and that at least 71% of cases were brought against women who were economically disadvantaged.¹¹⁹ In a world with little data privacy, where individuals may not have access to legal abortion, these tragic stories will occur more often.

Additionally, any semblance of privacy that one can retain will be more available to socio-economically advantaged individuals. Securing personal privacy is not only difficult, but expensive.¹²⁰ Technology protections, such as virtual private networks (VPNs) that encrypt data and make it more difficult for information to be tracked and linked, often cost money.¹²¹ Choosing products that are less likely to sell a user's data may be more expensive. Thus, those most able to limit their data sharing will likely also be those with the disposable income to afford these choices. The disparate impacts of harms is worrisome within the reproductive health data ecosystem, but in the post-*Dobbs* era in which we now find ourselves, the potential criminalization of reproductive health coupled with lack of reproductive data privacy becomes downright chilling.

C. Privacy Regulation (or a Lack Thereof)

Despite the broad sharing and selling of personal reproductive health information in U.S. society, federal law only minimally protects the privacy of such information.¹²² Health privacy in the United States is regulated by HIPAA.¹²³ HIPAA regulates “[p]rotected health information” and sets rules governing how such information can be shared.¹²⁴ The definition of “protected health information” is broad enough to include all sorts of reproductive health information, from use of contraception to pregnancy and pregnancy loss to

¹¹⁸ See *infra* Subsection II.B.1; see also PREGNANCY JUST., CONFRONTING PREGNANCY CRIMINALIZATION: A PRACTICAL GUIDE FOR HEALTHCARE PROVIDERS, LAWYERS, MEDICAL EXAMINERS, CHILD WELFARE WORKERS, AND POLICYMAKERS 5, 9 (2022) (tracking more than 1,700 cases of criminalization of pregnancy pre-*Dobbs*, with cases disproportionately targeting low-income women and women of color).

¹¹⁹ Paltrow & Flavin, *supra* note 117, at 311.

¹²⁰ See *infra* Section IV.A (discussing how difficult it is to self-manage privacy).

¹²¹ Elvy, *supra* note 78, at 1390.

¹²² Richard Sobel, *The HIPAA Paradox: The Privacy Rule That's Not*, HASTINGS CTR. REP., July–Aug. 2007, at 40, 40 (explaining the limitations and narrow scope of HIPAA).

¹²³ See generally Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936; 45 C.F.R. pt. 160 (2021); *id.* pt. 164 subpts. A, E.

¹²⁴ 45 C.F.R. § 160.103. Protected health information includes “individually identifiable health information” that “[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual” *Id.* Protected health information includes most “individually identifiable information” as defined here. *Id.*

abortion services.¹²⁵ HIPAA, however, only applies to health plans, healthcare clearinghouses, healthcare providers, and business associates.¹²⁶ Thus, the siloed nature of the law means that health information outside of the healthcare space is not similarly protected.¹²⁷

Indeed, there is no broad federal privacy law that protects sensitive health information, including reproductive health information, outside of the healthcare setting.¹²⁸ What's more, HIPAA does not regulate the vast amount of personal data that can be used to infer an individual's health status.¹²⁹ Thus, beyond HIPAA protections, there are relatively few restrictions on the amount of personal data that can be collected and shared.¹³⁰ Nevertheless, the public often believes that the law offers much greater protection of sensitive health

¹²⁵ See *id.*

¹²⁶ *Id.* pt. 160; *id.* § 164.104(a)–(b). Congress amended HIPAA in 2009 through the Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226, 467, which was included in the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115. HITECH extended HIPAA regulations to business associates of covered entities. HITECH Act §§ 13401, 13408. A business associate is defined as:

[A] person who . . . creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities . . . , billing, benefit management, practice management, and repricing; or . . . [who] [p]rovides . . . legal, actuarial, accounting, consulting, data aggregation . . . , management, administrative, accreditation, or financial services to or for such covered entity . . .

45 C.F.R. § 160.103.

¹²⁷ Terry, *supra* note 71, at 162–73 (noting the ways that HIPAA fails to protect healthcare-related data); Lisa Bari & Daniel P. O'Neill, *Rethinking Patient Data Privacy in the Era of Digital Health*, HEALTH AFFS. (Dec. 12, 2019), <https://www.healthaffairs.org/doi/10.1377/forefront.20191210.216658/full/> [<https://perma.cc/QU67-2RZM>] (discussing how digital health complicates existing health privacy protections); Price et al., *supra* note 49, at 448–49 (illuminating the worrying trend of companies establishing shadow health records outside the bounds of HIPAA protection); W. Nicholson Price II & I. Glenn Cohen, *Privacy in the Age of Medical Big Data*, 25 NATURE MED. 37, 39 & fig.2 (2019); W. Nicholson Price II, *Problematic Interactions Between AI and Health Privacy*, 2021 UTAH L. REV. 925, 926–28.

¹²⁸ See generally Sobel, *supra* note 122 (discussing various gaps in HIPAA that limit its ability to broadly protect health information privacy). See Fowler & Morain, *supra* note 13, at 204, 209–11 (noting that HIPAA does not protect Femtech apps, but that there may be other rules, such as mobile phone app store rules or state laws, that constrain a company's privacy practices).

¹²⁹ See, e.g., Prince, *supra* note 47, at 48 (noting that HIPAA does not protect health data that can be inferred from location information); Terry, *supra* note 71, at 147 (highlighting the problem created by HIPAA not protecting “medically inflected” data); Marks, *supra* note 47, at 997 (labelling this type of data as “emergent medical data”).

¹³⁰ This is not to say that HIPAA is powerless. For example, in their recent article, Professors David Cohen, Greer Donley, and Rachel Rebouché discuss ways that HIPAA could be used to further protect reproductive health information from access by law enforcement. David S. Cohen, Greer Donley & Rachel Rebouché, *The New Abortion Battleground*, 123 COLUM. L. REV. 1, 77–79 (2023).

information than it actually does.¹³¹ This may lead individuals to disclose health information to companies under the assumption that the data are more protected than they are.¹³²

Although there is not yet a broad federal data privacy law that protects sensitive information no matter where it is stored, there are some rules regarding how companies must interact with individuals and their personal data.¹³³ For example, companies must honor promises made to customers in user agreements about how personal data will be collected and used. The policies are often filled with jargon and legalese, making them difficult for the average person to understand.¹³⁴ Unsurprisingly, most users agree to these privacy policies without reading them.¹³⁵ The agreements, however, are important because once the company standards have been laid out, the FTC or relevant state attorney general can undertake enforcement measures for unfair and deceptive practices if companies do not honor the agreements.¹³⁶

Such enforcement measures can lead to meaningful changes regarding unjustified data practices. For example, in 2021, the FTC sued Flo Health, Inc. (Flo), a popular Femtech app used by millions of women, including sixteen million users in the United States.¹³⁷ Flo collected information about menstrual cycles, pregnancies and pregnancy results, and reproductive health symptoms.¹³⁸ Flo's privacy policies specifically told users that the company would not share "any data related to health" with third parties.¹³⁹ In reality, Flo regu-

¹³¹ Matthew T. Bodie, *HIPPA*, 43 CARDOZO L. REV. DE NOVO 118, 121–23 (2022), http://cardozolawreview.com/wp-content/uploads/2022/04/BODIE_DN_43_PUBLISH.pdf [<https://perma.cc/AJ6C-DTQ5>] (highlighting how individuals often mistake HIPAA as protecting health information disclosure in all arenas despite efforts to educate the public that this is not the case).

¹³² This misconception about health privacy specifically is just one aspect of a larger problem where individuals regularly incorrectly believe that their data is more private than it actually is. Solove, *supra* note 69, at 1886 (noting, among other statistics, that seventy-five percent of individuals surveyed in a study incorrectly believed that if a website has a privacy policy it means that the company will not share their data (citing JOSEPH TUROW, LAUREN FELDMEN & KIMBERLY MELTZER, ANNENBERG PUB. POL'Y CTR., OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE 3 (2005))).

¹³³ See Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598–99 (2014).

¹³⁴ Gilman, *supra* note 11, at 110.

¹³⁵ Solove, *supra* note 69, at 1884.

¹³⁶ See, e.g., Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 107 (2021); see also Solove, *supra* note 69, at 1884 (noting that the "FTC has stepped in to serve as an enforcer of privacy notices").

¹³⁷ Complaint at 1–2, Flo Health, Inc., No. C-4747 (F.T.C. June 17, 2021); 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/P9S9-DAML>].

¹³⁸ Complaint, *supra* note 137, at 1.

¹³⁹ *Id.* at 3 (emphasis omitted).

larly shared users' reproductive health data with third-party companies, such as Facebook (now Meta), Google, and other marketing and analytics firms,¹⁴⁰ without placing any limits on how these third parties could use the data.¹⁴¹ Flo later settled with the FTC, agreeing to stop misrepresenting their data practices and promising to get affirmative consent from their users before sharing health information with third parties.¹⁴² Notably, the settlement did not actually constrain Flo from widely sharing data with third parties despite evidence presented in the complaint that individuals felt their reproductive health information should be private.¹⁴³

Yet, as *Flo Health, Inc.* shows, regulatory enforcement can lead companies to improve their privacy practices. Indeed, the FTC has continued to be active in this space in recent years.¹⁴⁴ In August 2022, for instance, the FTC sued a data broker, Kochava Inc., for selling geolocation data that could trace individuals' traffic to sensitive locations, including reproductive health clinics.¹⁴⁵ In the same month, the FTC posted an advance notice of proposed rulemaking (ANPR) that requested public comment on commercial surveillance and ways to regulate these practices.¹⁴⁶ Although this ANPR is not specifically focused on reproductive health, if done well, it may engender important changes in privacy regulation that bolster reproductive privacy.

¹⁴⁰ *Id.* at 4.

¹⁴¹ *Id.* at 5.

¹⁴² Press Release, Fed. Trade Comm'n, Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations That It Misled Consumers About the Disclosure of Their Health Data (Jan. 13, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about> [<https://perma.cc/8CH5-RCN3>].

¹⁴³ Complaint, *supra* note 137, at 5–6 (emphasizing quotations from upset Flo users, such as “[t]his is private personal data and I feel disgusted that you are now making this data available to third parties” and “[w]hy would you EVER think it is ok to share that personal, private information with a third [sic] party” (third alteration in original)); see also Solow-Niederman, *supra* note 71, at 376 (noting that FTC enforcement does not “fundamentally alter[] the underlying regulatory regime”). Others have found certain aspects of FTC enforcement, such as the Health Breach Notification Rule, to be good, but not perfect. See Fowler & Ulrich, *supra* note 26 (manuscript at 47–48).

¹⁴⁴ The FTC has been one of the primary regulators of privacy in the United States, outside of HIPAA enforcement. See generally Solove & Hartzog, *supra* note 133, at 590.

¹⁴⁵ Complaint for Permanent Injunction & Other Relief at 1, Fed. Trade Comm'n v. Kochava Inc., No. 2:22-cv-377 (D. Idaho Aug. 29, 2022); Press Release, Fed. Trade Comm'n, 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/RJ6J-LCS9>].

¹⁴⁶ Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51273 (proposed Aug. 22, 2022).

State law sometimes adds additional protections beyond enforcement of unfair trade practices.¹⁴⁷ In some states, companies are required to provide consumers with specific notices about data practices. For example, the California Consumer Privacy Act of 2018 (CCPA) requires companies to give notice regarding the personal information collected, the purposes for which it will be used, and the company's privacy policies.¹⁴⁸ Consumers also have the right to opt out of company practices to sell their data and a link to make this request must also be included in the initial notice.¹⁴⁹

Nevertheless, FTC enforcement and state laws like the CCPA are by no means a panacea.¹⁵⁰ Neither option circumscribes what data can be collected, how they can be analyzed, and with whom they can be shared.¹⁵¹ Instead, unfair trade practice laws simply require the company to comply with the privacy policies that the company itself establishes. Similarly, the CCPA requires companies to disclose their data practices without limiting what these practices are.¹⁵² Given the profits that can be made from the sale of personal data,¹⁵³ especially data related to reproductive health,¹⁵⁴ companies do not have the economic motivation to self-regulate in meaningful ways.¹⁵⁵

¹⁴⁷ Just as the FTC has impacted privacy regulation through enforcement, state attorneys general have also been key actors in privacy law at the state level. *See generally* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016) (discussing the role of state attorneys general in developing privacy regulations).

¹⁴⁸ CAL. CIV. CODE §§ 1798.115, 1798.120(b) (West 2023); CAL. CODE REGS. tit. 11, § 7012(b) (2023).

¹⁴⁹ CAL. CIV. CODE § 1798.120(a) (“A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer’s personal information. This right may be referred to as the right to opt-out of sale or sharing.”). Regardless of consumer preferences, the law prohibits selling or sharing personal information “if the business has actual knowledge that the consumer is less than 16 years of age” unless the consumer or their guardian (depending on age) affirmatively opts into this practice. *Id.* § 1798.120(c).

¹⁵⁰ *See, e.g.*, Jake Holland, *Abortion Access Data and State Consumer Privacy Laws: Explained*, BLOOMBERG L. (July 11, 2022), <https://news.bloomberglaw.com/privacy-and-data-security/abortion-access-data-and-state-consumer-privacy-laws-explained> [<https://perma.cc/GVD8-4AYB>] (briefly explaining new state privacy laws and their protections and exceptions as they relate to abortion laws).

¹⁵¹ *See* CAL. CIV. CODE § 1798.100(a)(1) (requiring a business that collects the personal information of a consumer to inform the consumer, but not forbidding actual collection); Gilman, *supra* note 11, at 110 (noting that “the FTC’s regulatory powers can only focus on broken promises, and cannot give bite to the notion of consumer consent”).

¹⁵² CAL. CIV. CODE § 1798.100(a)(1).

¹⁵³ Elvy, *supra* note 78, at 1373 (“[C]ompanies have developed various approaches to monetizing consumer data and privacy to exploit the rising data gold rush . . .”).

¹⁵⁴ *See generally* Gilman, *supra* note 11 (exploring the surveillance and monetization of reproductive health).

¹⁵⁵ *But see* Prince, *supra* note 47, at 86–87 (noting, however, that there are some companies that are engaging in more privacy by design as part of their business model).

II. THE CHANGING REPRODUCTIVE HEALTH LANDSCAPE

On June 24, 2022, in *Dobbs v. Jackson Women's Health Organization*, the U.S. Supreme Court overruled *Roe v. Wade*, taking away women's constitutional right to an abortion and sending regulation of abortion back to the states.¹⁵⁶ Although the *Dobbs* decision sets women's reproductive rights back fifty years, medical and technological advancements place pregnant individuals in a very different world than they were in prior to *Roe*. Given increasing restrictions on abortion and the intertwined nature of reproductive health outcomes, this Part presents how these medical advances¹⁵⁷ and legal changes¹⁵⁸ will impact all aspects of reproductive health and its associated data ecosystem.

A. Medical Landscape

In particular, two significant reproductive medical advances have increased in relevance following the *Dobbs* decision: medication abortion¹⁵⁹ and assisted reproductive technology (ART).¹⁶⁰ Although medication abortion is used to help terminate a pregnancy or manage a miscarriage, ART is used to help individuals grow a family or preserve fertility. Nevertheless, as this Section discusses, post-*Dobbs*, both are increasingly in the law's crosshairs.¹⁶¹ Additionally, the two are much more entwined than may initially appear.¹⁶²

1. Medication Abortion

Medication abortion, sometimes referred to as the "abortion pill," is a Food and Drug Administration (FDA) approved two-drug regimen of mifepristone and misoprostol.¹⁶³ The use of medication abortion has greatly increased

¹⁵⁶ *Dobbs*, 142 S. Ct. 2228, 2242 (2022); *Roe*, 410 U.S. 113 (1973), overruled by *Dobbs*, 142 S. Ct. 2228.

¹⁵⁷ See *infra* Section II.A.

¹⁵⁸ See *infra* Section II.B.

¹⁵⁹ See *infra* Subsection II.A.1.

¹⁶⁰ See *infra* Subsection II.A.2.

¹⁶¹ See *infra* Section II.A.

¹⁶² See *infra* Subsection II.A.3.

¹⁶³ Rachel K. Jones et al., *Medication Abortion Now Accounts for More Than Half of All US Abortions*, GUTTMACHER INST., <https://www.guttmacher.org/article/2022/02/medication-abortion-now-accounts-more-half-all-us-abortions> [<https://perma.cc/R644-W74X>] (Dec. 1, 2022). The drug combination is incredibly safe and effective. *Id.* Indeed, some safety data shows that it has a lower fatality rate than pregnancy-related complications for those choosing to proceed to live birth. See Greer Donley, *Medication Abortion Exceptionalism*, 107 CORNELL L. REV. 627, 634 (2022). See generally Cohen et al., *supra* note 29 (discussing legal issues related to medication abortion in a post-*Dobbs* world).

in recent years because of regulatory changes at the federal level.¹⁶⁴ The number of individuals accessing abortion using medication now accounts for over half of all abortions in the United States.¹⁶⁵

Access to abortion medication, specifically mifepristone, is currently under threat through lawsuits and state legislation.¹⁶⁶ For example, as of December 2022, nineteen states bar telehealth prescription of medication abortion, thus requiring an in-person visit to a physician.¹⁶⁷ Post-*Dobbs*, states will likely continue to impose restrictions on medication abortion, either through complete bans on abortion altogether or targeted restrictions on medication abortion.¹⁶⁸

Whether these restrictions can effectively stop abortions through medication is a different question. “Though illegal abortion conjures up images of the back-alley abortions from generations ago, self-managed abortion in today’s world is very different.”¹⁶⁹ In some instances, a pregnant individual from a

¹⁶⁴ Jones et al., *supra* note 163 (documenting the increased use of medication abortion since 2000). One drug in the combination, mifepristone, has been heavily regulated by the FDA, creating barriers to access. *See generally* Donley, *supra* note 163 (explaining how the Risk Evaluation and Mitigation Strategy (REMS) has limited the availability of the drug mifepristone). During the COVID-19 pandemic, however, a court-ordered injunction resulted in access to mifepristone prescriptions without an in-person visit to a clinic. *Id.* at 650. This injunction was short-lived—the Supreme Court reverted to in-person dispensing requirements—but it lasted long enough to facilitate gathering further data about the safety of the medication when prescribed via telehealth. *Id.* Based in part on this new data, in December 2021, the Biden Administration FDA permanently ended the federal in-person requirement to obtain a mifepristone prescription. *Id.* at 642, 650. This has expanded the availability of abortion services and increased the percentage of abortions via medication. Jones et al., *supra* note 163. Following the *Dobbs* decision, the Biden Administration continued efforts to increase access to medication abortion, such as by formalizing the rule allowing medication to be distributed by large-scale pharmacies in January 2023. Cohen et al., *supra* note 29 (manuscript at 6–8). The second drug in the combination, misoprostol, is not as heavily regulated, so the medication has been more accessible. Donley, *supra* note 163, at 634. This is likely because the drug has other medical uses and can be prescribed for reasons other than to induce abortions. *Id.* at 633–34. Increasing abortion restrictions across the country, however, may result in misoprostol becoming more difficult to access for abortion and non-abortion purposes alike. For example, there have been reports that patients in Texas have had difficulty filling prescriptions for misoprostol to treat miscarriages since abortion restrictions went into effect in the state in 2021. Charlotte Huff, *In Texas, Abortion Laws Inhibit Care for Miscarriages*, NPR (May 10, 2022), <https://www.npr.org/sections/health-shots/2022/05/10/1097734167/in-texas-abortion-laws-inhibit-care-for-miscarriages> [<https://perma.cc/5945-UDH6>].

¹⁶⁵ Jones et al., *supra* note 163.

¹⁶⁶ This is a rapidly changing landscape with many lawsuits, administrative decisions, and state legislation developing in tandem. *See generally* Cohen et al., *supra* note 29 (highlighting key legal updates regarding abortion medication following *Dobbs*). *See also* Medication Abortion Requirements, POL’Y SURVEILLANCE PROGRAM, <https://lawatlas.org/datasets/medication-abortion-requirements> [<https://perma.cc/CH5Q-3PKB>] (Nov. 1, 2022).

¹⁶⁷ Jones et al., *supra* note 163.

¹⁶⁸ Brendan Pierson & Nate Raymond, *Explainer: Can Abortion Pills Overcome U.S. State Bans?*, REUTERS (June 24, 2022), <https://www.reuters.com/world/us/can-abortion-pills-overcome-us-state-bans-2022-06-24/> [<https://perma.cc/756T-ZGHS>]; *see also* Medication Abortion Requirements, *supra* note 166.

¹⁶⁹ Donley, *supra* note 163, at 695.

state with abortion restrictions may be able to access medication abortion via out-of-state providers.¹⁷⁰ In others, international organizations offer prescriptions that can be mailed to pregnant individuals¹⁷¹—thus thwarting the legal restrictions of the FDA¹⁷² and states attempting to limit abortion. As more states increase restrictions on both surgical and medication abortions post-*Dobbs*, the number of individuals seeking to self-manage their abortions is likely to increase.¹⁷³ Indeed, internet searches for abortion medication are associated with greater restrictions on abortions¹⁷⁴—a trend that continued with the *Dobbs* decision.¹⁷⁵

Abortion medication creates the possibility that many women can access safe abortions in the comfort of their homes.¹⁷⁶ The medications can be cheaper than alternatives, are more accessible for low-income individuals and those living in rural communities, and can help individuals avoid the harassment often associated with a visit to an abortion clinic.¹⁷⁷ But accessing medication abortion still requires online interactions, such as internet searches and virtual contact with providing companies.¹⁷⁸ These interactions leave plenty of virtual bread crumbs regarding reproductive status and intent to terminate a pregnancy.

¹⁷⁰ *The Plan C Guide to Abortion Pill Access*, PLAN C, <https://www.plancpills.org/find-pills> [<https://perma.cc/FUV5-ES6W>] (providing guidance on how to receive at-home abortion care regardless of which state you live in); Donley, *supra* note 163, at 696; *see also* Cohen et al., *supra* note 29 (manuscript at 9) (noting that abortion medication legally prescribed in one state via telehealth may be carried across state lines to be ingested in a state with restrictions).

¹⁷¹ *See* Donley, *supra* note 163, at 660.

¹⁷² *See, e.g.*, Warning Letter from Thomas Christi, Dir., Off. of Drug Sec., Integrity & Response, Food & Drug Admin., to Aidaccess.org (Mar. 8, 2019), <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/aidaccessorg-575658-03082019> [<https://perma.cc/KF5T-NTX8>].

¹⁷³ *See* Haley Ott, *European Doctor Who Helps Americans Get Abortions Says She's Receiving 4,000 Inquiries a Day Since Roe v. Wade Overturned*, CBS NEWS (June 30, 2022), <https://www.cbsnews.com/news/doctor-rebecca-gomperts-helps-americans-abortions-reports-4000-inquiries-since-roe-overturned/> [<https://perma.cc/3BAY-BVA5>].

¹⁷⁴ *See generally* Sylvia Guendelman et al., *Shining the Light on Abortion: Drivers of Online Abortion Searches Across the United States in 2018*, PLOS ONE, May 21, 2020, at 1, 1 (exploring trends in internet searches for abortion medications).

¹⁷⁵ Adam Poliak et al., *Internet Searches for Abortion Medications Following the Leaked Supreme Court of the United States Draft Ruling*, 182 JAMA INTERNAL MED. 1002, 1003 (2022) (exploring trends in internet searches for abortion medications after the leaked *Dobbs* draft).

¹⁷⁶ As Professor Donley notes, involvement of a healthcare provider is “the gold standard” for abortion care, but self-managed abortion can still be undertaken safely. Donley, *supra* note 163, at 658–59.

¹⁷⁷ *Id.* at 691–92; *see also* Lindgren, *supra* note 117, at 344–45.

¹⁷⁸ As the then-host of the *Daily Show* Trevor Noah quipped, “How are you going to search for abortion pills without Google? Why, you’re just gonna have to write a question on a piece of paper, throw it out the window and hope for the best?” Ron Dicker, *Trevor Noah Laments One Drastic Measure Women Have to Take After Roe Repeal*, HUFFPOST (June 30, 2022) (quoting Trevor Noah, Host, *The Daily Show*), https://www.huffpost.com/entry/trevor-noah-phone-period-tracking_n_62bdb7abe4b0ffe00a0edac [<https://perma.cc/5HBY-SBLK>].

2. Assisted Reproductive Technologies (ART)

The Supreme Court decided *Roe v. Wade* in 1973.¹⁷⁹ Just five years later, the first child was born using IVF, one of the most widely-used forms of ART.¹⁸⁰ Since its development, ART has become increasingly common in the United States. Approximately 13% of women between the ages of fifteen and forty-nine have sought out fertility care and, in 2019, approximately 84,000 children—or 2.2% of all babies—were born using IVF.¹⁸¹

Although millions of children have been born using ART, the process remains complicated.¹⁸² Throughout the process of fertilization, early growth, and sometimes, genetic testing, some fertilized eggs may be discarded or fail to develop.¹⁸³ Even after this process, it is common to have several fertilized embryos and freeze those that are not implanted.¹⁸⁴ These cryopreserved embryos may be used by the patient in the future, donated to another individual or couple, or discarded.¹⁸⁵

Just as with medication abortion, ART does not occur in an information vacuum. Individuals undergoing ART may search for questions online, have location data showing multiple trips to fertility clinics, or changes in purchasing habits. These bread crumbs that show an intent to start or grow a family will be collected by the reproductive health data ecosystem.

¹⁷⁹ See generally 410 U.S. 113 (1973), *overruled by* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022).

¹⁸⁰ Carlos Wilson Dala Paula Abreu Abreu et al., *Final Destination of Surplus Cryopreserved Embryos. What Decision Should be Made?*, 25 JBRA ASSISTED REPROD. 276, 276 (2021); CDC, 2019 ASSISTED REPRODUCTIVE TECHNOLOGY: FERTILITY CLINIC AND NATIONAL SUMMARY REPORT 2 (2021).

¹⁸¹ CDC, *supra* note 180, at 2; Eve C. Feinberg, Jennifer F. Kawwass & Marcelle I. Cedars, *Roe v. Wade and the Threat to Fertility Care*, 140 OBSTETRICS & GYNECOLOGY 557, 557 (2022). The number of ART cycles in the country has doubled in just ten years. CDC, *supra* note 180, at 32.

¹⁸² Abreu et al., *supra* note 180, at 276.

¹⁸³ ART: Step-by-Step Guide, SOC'Y FOR ASSISTED REPROD. TECH., <https://www.sart.org/patients/a-patients-guide-to-assisted-reproductive-technology/general-information/art-step-by-step-guide/> [<https://perma.cc/9RVT-4G2R>]; Feinberg et al., *supra* note 181, at 558–59 (noting that “[e]mbryonic loss is a routine part of nature and occurs from fertilization onward both in vivo and in vitro and manifests as failed blastocyst development, failed implantation, or miscarriage”).

¹⁸⁴ *In Vitro Fertilization (IVF)*, MAYO CLINIC, <https://www.mayoclinic.org/tests-procedures/in-vitro-fertilization/about/pac-20384716> [<https://perma.cc/9BHU-BGZK>].

¹⁸⁵ *Id.*; see also I. Glenn Cohen, *Reproductive Technologies and Embryo Destruction After Dobbs* 2 (Harv. Pub. L. Working Paper, Paper No. 23-03, 2022), <https://ssrn.com/abstract=4284007> [<https://perma.cc/XP9P-9P22>] (noting that “[w]hen it comes to In Vitro Fertilization (IVF), embryo destruction is very common”).

3. Blurring Distinctions

At first blush, the technological advances of medication abortion and ART may seem entirely distinct—one is used to end a pregnancy, the other is used to begin one. Both advances, however, highlight the complex ways that various aspects of reproductive healthcare intersect. These blurring distinctions serve to make the reproductive health data ecosystem all the more problematic.

For example, there is remarkable overlap between abortion and pregnancy loss.¹⁸⁶ To begin with, the medical and physical experiences can be similar.¹⁸⁷ If a woman has experienced an “incomplete” miscarriage, she may be prescribed misoprostol, one of the two medications used in medication abortion.¹⁸⁸ If miscarriage or stillbirth occurs later in pregnancy, a woman may undergo surgical procedures that are the same as abortion surgical procedures.¹⁸⁹ Although those who experience miscarriage may have lost a wanted pregnancy and those who undergo abortion may have an unintended pregnancy, this will not always be the case—some experiencing miscarriage may feel relief and some who want a child may make the choice to terminate due to the health of the fetus or mother.¹⁹⁰ Additionally, both miscarriages and abortions are extremely common, given that roughly 15% of known pregnancies end in pregnancy loss and approximately 20% of pregnancies end in abortion.¹⁹¹

Similarly, the line between fertility care and abortion has become murky, especially in discussions about when life begins. For example, some anti-abortion activists seek to define life as beginning at “conception” or “fertilization.”¹⁹² But if one takes the view that life begins when a sperm fertilizes an egg, many aspects of ART procedures and large numbers of cryopreserved embryos currently in storage would be implicated.¹⁹³

¹⁸⁶ See Donley & Lens, *supra* note 1, at 1662–76 (discussing in detail the “[s]urprising [o]verlap [b]etween [a]bortion and [p]regnancy [l]oss”).

¹⁸⁷ *Id.* at 1662–63.

¹⁸⁸ Donley, *supra* note 163, at 662. Recent research has indicated that receiving both mifepristone and misoprostol may be more effective in managing miscarriage, thus making miscarriage even more medically similar to medication abortion. *Id.*

¹⁸⁹ Donley & Lens, *supra* note 1, at 1667.

¹⁹⁰ See *id.* at 1676 (explaining that “[w]omen are not a monolith in either group”).

¹⁹¹ See *supra* notes 1–2 and accompanying text (detailing the frequency of pregnancy loss and termination).

¹⁹² Feinberg et al., *supra* note 181, at 558–59 & tbl.2 (discussing “personhood” bills that have been introduced in state legislatures).

¹⁹³ *Id.*; Mindy S. Christianson et al., *Embryo Cryopreservation and Utilization in the United States from 2004–2013*, FERTILITY & STERILITY REPS., Sept. 2020, at 71, 73 (noting that between 2004 and 2013 almost 2 million embryos were cryopreserved and fewer than 750,000 of those were transferred during that period); Cohen, *supra* note 185, at 2 (arguing that it is actually easier to justify restrictions of embryo destruction than restrictions on abortion).

Given these blurred distinctions between various aspects of reproduction, the health data collected about individuals may look remarkably similar. Women experiencing pregnancy loss or seeking to terminate may both research information about the drugs used in medication abortion. They may both send text messages discussing no longer being pregnant. Women across a number of reproductive health experiences, from abortion to pregnancy loss to IVF, will also share similar data patterns. They may all have location data showing their arrival at a health clinic. They may all have behavioral data indicating pregnancy, such as purchasing of a pregnancy test, then have behavioral data indicating they are no longer pregnant, such as resuming the consumption of alcohol. Even an individual undergoing various rounds of IVF may have on-again, off-again behavior that looks more like pregnancy or termination if they change behaviors during cycles or if there is an implantation that does not take. As will be discussed further in the next Section, the rapidly changing legal landscape makes these reproductive data a liability for all who can get pregnant.¹⁹⁴

B. Legal Landscape

Following *Dobbs*, states are increasingly restricting or banning pregnancy termination, opening up individuals to criminal and civil liability.¹⁹⁵ Unfortunately, this criminal prosecution of and discrimination against pregnancy behaviors and outcomes is not new.¹⁹⁶ As this Section discusses, *Dobbs* will only increase historical practices of punishing women for pregnancy outcomes, especially in marginalized communities. Furthermore, the rapidly changing legal landscape following *Dobbs* has the potential to impact all aspects of reproductive health by increasing legal risk and chilling behaviors.¹⁹⁷

1. Targeting Pregnant Individuals

Reproductive health has long been under criminal scrutiny, even before *Roe* was overturned.¹⁹⁸ Many prosecutorial efforts have focused on suspected pregnancy termination, but others have focused on behaviors during pregnancy.¹⁹⁹ For example, prosecutors have brought charges alleging child abuse and homicide, among other crimes, often when there has been evidence of drug use

¹⁹⁴ See *infra* Section II.B (discussing the current legal landscape surrounding reproductive data).

¹⁹⁵ See *infra* Subsection II.B.1.

¹⁹⁶ See *infra* Subsection II.B.1.

¹⁹⁷ See *infra* Subsection II.B.2.

¹⁹⁸ See generally PREGNANCY JUST., *supra* note 118 (detailing the criminalization of pregnancy); GOODWIN, *supra* note 34 (discussing how reproduction has been policed in the United States and the disproportionate impacts of this state surveillance).

¹⁹⁹ PREGNANCY JUST., *supra* note 118, at 9–11.

during a pregnancy.²⁰⁰ In general, these laws were not originally intended to target pregnant women or those who have experienced pregnancy loss.²⁰¹ For example, some laws prohibiting fetal homicides or increasing penalties for crimes against pregnant women explicitly include maternal exceptions.²⁰² Nevertheless, prosecutors continue to bring cases against pregnant women.²⁰³

What's more, the criminalization of pregnancy and pregnancy loss is increasing rapidly. Pregnancy Justice reports that there have been over 1,700 cases related to the criminalization of pregnancy since 1973.²⁰⁴ These numbers include prosecutions for the actions of a woman during pregnancy, such as drug use, as well as prosecutions for suspected termination of pregnancy.²⁰⁵ The organization reports that there have been three times as many instances occurring in the fourteen years from 2006 to 2020 than in the thirty-two years from 1973 to 2005.²⁰⁶

These actions most often target marginalized communities, such as pregnant women of color, low-income individuals, and those who have used drugs.²⁰⁷ For example, despite similar rates of drug use, Black women are disproportionately more likely to be reported to authorities for suspected use during pregnancy.²⁰⁸ Due to systemic injustices, these populations are already more likely to have limited access to healthcare and prenatal services and

²⁰⁰ *Id.* at 9; Donley & Lens, *supra* note 1, at 1696, 1704 (noting, however, that there is little evidence linking drug use and pregnancy loss and in many prosecutions a healthy baby was born). See generally Paltrow & Flavin, *supra* note 117 (documenting a number of cases where pregnant women were arrested and/or had charges brought against them due to actions taken while pregnant).

²⁰¹ PREGNANCY JUST., *supra* note 118, at 5 (“With limited exceptions, the laws used to prosecute pregnancy-related crimes were never intended to encompass the actions of pregnant women in relation to their own pregnancies.”).

²⁰² Andrew S. Murphy, Comment, *A Survey of State Fetal Homicide Laws and Their Potential Applicability to Pregnant Women Who Harm Their Own Fetuses*, 89 IND. L.J. 847, 853 (2014) (noting that The Unborn Victims of Violence Act, a federal law, included an exception stating that the “prosecution . . . of any woman with respect to her unborn child” was not permitted under the law, and that many states utilized a similar exception in their own criminal laws (alteration in original) (citing 18 U.S.C. § 1841(c)(3))).

²⁰³ See, e.g., Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV. 1, 3–4 (2020). This is not to say that the law always includes a “maternal exception.” Murphy, *supra* note 202, at 853. For example, several states have fetal homicide laws that allow prosecution of a pregnant individual for the death of an unborn child. Donley & Lens, *supra* note 1, at 1695–96.

²⁰⁴ PREGNANCY JUST., *supra* note 118, at 5. Pregnancy Justice was previously known as the National Advocates for Pregnant Women. *Id.*

²⁰⁵ *Id.*

²⁰⁶ *Id.*

²⁰⁷ *Id.* at 7; Donley & Lens, *supra* note 1, at 1704; GOODWIN, *supra* note 34, at 122–23.

²⁰⁸ PREGNANCY JUST., *supra* note 118, at 20 (citing Ira J. Chasnoff, Harvey J. Landress & Mark E. Barrett, *The Prevalence of Illicit-Drug or Alcohol Use During Pregnancy and Discrepancies in Mandatory Reporting in Pinellas County, Florida*, 322 NEW ENG. J. MED. 1202 (1990)) (detailing a study wherein Black women were found ten times more likely to be reported to health authorities for drug use during pregnancy than white women despite similar rates of use).

greater interactions with the child welfare and criminal systems, further entrenching harm in these communities.²⁰⁹

2. Legislation Post-*Dobbs*

Even though criminalization and discrimination of pregnancy status and outcomes is not new, the quickly changing legal landscape post-*Dobbs* will only exacerbate the effects. Following *Dobbs*, state law is rapidly changing the legal landscape for abortion, and pregnancy termination is now banned or severely restricted in fourteen states.²¹⁰ As with laws related to pregnancy behaviors, abortion restrictions have generally focused on criminalizing or imposing civil penalties on the providers of abortions, not the pregnant individuals themselves.²¹¹ Indeed, historically, it was seen as unpalatable, even among those opposing abortion, to take aim at the individuals undergoing the procedures.²¹² With the growing availability and ease of medication abortion, however, pregnant individuals are increasingly able to terminate a pregnancy without an in-person visit to a provider and, sometimes, without any involvement of a U.S. provider.²¹³ States that wish to prohibit abortion will likely see the need to target self-managed abortion, and, therefore, increasingly the pregnant individuals themselves.²¹⁴

²⁰⁹ GOODWIN, *supra* note 34, at 114–28; *see also* KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 122 (2017) (speaking to the systematic injustices of the impoverished, including violations of privacy rights).

²¹⁰ In the days, weeks, and months following the *Dobbs* decision, states immediately began restricting abortion prior to viability, with some implementing a complete ban on abortion, usually with few exceptions. As of March 20, 2023, fourteen states have full or six-week abortion bans in effect. *Tracking the States Where Abortion Is Now Banned*, N.Y. TIMES, <https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html> [<https://perma.cc/V45W-J29F>] (Mar. 20, 2023). More states are expected to follow suit. For example, eight states currently have bans blocked by courts and litigation is pending in at least several of these states. *Id.* Additionally, the Guttmacher Institute is closely following state bills that impact abortion care during the 2023 state legislative sessions. *State Legislation Tracker: Major Developments in Sexual & Reproductive Health*, GUTTMACHER INST., <https://www.guttmacher.org/state-legislation-tracker> [<https://perma.cc/6YAL-NP8S>] (Apr. 15, 2023).

²¹¹ Michelle Oberman, *Abortion Bans, Doctors, and the Criminalization of Patients*, HASTINGS CTR. REP., Mar.–Apr. 2018, at 5, 5 (“Historically, and in most countries today, abortion crimes typically are prosecuted against doctors, not women.”).

²¹² *Id.* (noting that anti-abortion advocates thought of those getting abortions as “second victims” who “deserv[e] compassion”).

²¹³ The latter option is not legal in the United States, as medication abortion must legally be obtained via FDA protocols and is barred in some states. Still, pregnant individuals may be able to access medication abortion online and through the mail—sometimes even from international companies. *See supra* Subsection II.A.1.

²¹⁴ There are currently only three states with laws that apply criminal penalties to an individual who self-manages an abortion. Cohen et al., *supra* note 29 (manuscript at 27). Yet criminal cases have been brought against individuals for self-managing abortion, disproportionately targeting people of color and those with low income. LAURA HUSS, FARAH DIAZ-TELLO & GOLEEN SAMARI, IF/WHEN/HOW, SELF-

Furthermore, *Dobbs* opens up the possibility of greater restrictions on contraceptives²¹⁵ and IVF.²¹⁶ For example, between 2020 and 2022, twenty-seven bills in eleven states proposed to define personhood as beginning at fertilization.²¹⁷ Although none of these bills were enacted,²¹⁸ there will likely be continued efforts at redefining personhood. Key aspects of IVF, such as cryo-preservation and embryo selection, could run afoul of state abortion restrictions depending on how they are written.²¹⁹ Indeed, it is clear that some anti-abortion activists desire and are actively strategizing for these restrictions on contraceptives and IVF.²²⁰ Already, this is causing individuals and families to change their reproductive plans, such as requesting that stored embryos following IVF be moved to states less likely to have restrictions.²²¹ As the next Part will show, given this changing landscape and increasing restrictions on reproductive choices, the issues regarding reproductive health data's lack of privacy will continue to be pertinent for individuals and families across the country.²²²

III. PENALIZING REPRODUCTIVE HEALTH & THE DATA ECOSYSTEM

Just as there have been significant medical and legal changes since *Roe v. Wade*, the informational landscape has also transformed. The ecosystem that regularly collects and infers the reproductive health information of individuals simply did not exist fifty years ago. This does not mean that women and their providers were historically immune from the use of personal data to target re-

CARE, CRIMINALIZED: AUGUST 2022 PRELIMINARY FINDINGS 2 (2022); see also Donley & Lens, *supra* note 1, at 1665–67 (noting that this will also implicate those who experience pregnancy loss because medication abortion is medically similar to a miscarriage).

²¹⁵ Zita Lazzarini, *The End of Roe v. Wade—States' Power Over Health and Well-Being*, 387 NEW ENG. J. MED. 390, 391 (2022).

²¹⁶ I. Glenn Cohen, Judith Daar & Eli Y. Adashi, Opinion, *What Overturning Roe v. Wade May Mean for Assisted Reproductive Technologies in the US*, 328 JAMA 15, 15–16 (2022) (discussing the ways that the *Dobbs* decision could affect ART, including IVF); see also Feinberg et al., *supra* note 181, at 558–59.

²¹⁷ Feinberg et al., *supra* note 181, at 558 tbl.2.

²¹⁸ *Id.*

²¹⁹ *Id.* at 558–59; Cohen et al., *supra* note 216, at 15–16.

²²⁰ Kavitha Surana, “We Need to Defend This Law”: Inside an Anti-abortion Meeting with Tennessee’s GOP Lawmakers, PROPUBLICA (Nov. 15, 2022), <https://www.propublica.org/article/inside-anti-abortion-meeting-with-tennessee-republican-lawmakers> [<https://perma.cc/7D5E-69LZ>] (detailing an anti-abortion strategy call in Tennessee where advocates encouraged greater restrictions).

²²¹ Katie Palmer & Casey Ross, *Health Tech Companies Are Scrambling to Close Data Privacy Gaps After Abortion Ruling*, STAT (July 2, 2022), <https://www.statnews.com/2022/07/02/roe-abortion-flo-clue-data-privacy/> [<https://perma.cc/RJ25-DDR7>]. Beyond just patients, companies that offer fertility- and IVF-related services are carefully tracking the laws and preparing for legal requests to access information about embryos. *Id.*

²²² See *infra* Part III.

productive health decisions.²²³ The breadth and depth of information available about reproductive health choices, however, has grown exponentially in the past fifty years. As this Part delineates, efforts to penalize reproductive health through criminalization,²²⁴ civil liability,²²⁵ and discrimination²²⁶ are fueled by easy access to the reproductive health data ecosystem.

A. Law Enforcement Access to Reproductive Health Data

Law enforcement may initiate investigations regarding pregnancy and pregnancy termination for a wide variety of reasons. Using abortion as an example, this Section discusses the robust ways that investigators and prosecutors use the reproductive health data ecosystem.²²⁷ As restrictions on reproductive health continue to grow, law enforcement access to data has implications for all who can get pregnant.²²⁸

1. Reports and Dragnets

In some instances, law enforcement may be keyed into a suspected abortion if an individual who undertakes medication abortion experiences a complication.²²⁹ In other cases, a friend or acquaintance could report an individual. In these cases, information from cellphones and internet searches has been used as evidence in the subsequent prosecution—a practice that could become “standard protocol” in jurisdictions where abortion is criminalized.²³⁰

Thus, at an individual level, a woman’s digital footprint could be the integral evidence that transforms a suspicion of self-managed abortion into a triable case. Take, for instance, the story of Latice Fisher, a woman investigated after paramedics brought her and her stillborn fetus to the hospital.²³¹ The

²²³ See *infra* Section III.B.

²²⁴ See *infra* Section III.A.

²²⁵ See *infra* Section III.B.

²²⁶ See *infra* Section III.C.

²²⁷ See *infra* Subsection III.A.1.

²²⁸ See *infra* Subsection III.A.2.

²²⁹ Although medication abortion has been proven safe, in about one percent of cases, the individual may experience an incomplete abortion and seek follow-up medical care, typically a surgical procedure. Donley & Lens, *supra* note 1, at 1706–07. In rare instances, there are other complications that necessitate medical follow-ups. *Id.* at 1706 (noting that “closer to five percent will seek out additional medical care” (citing Greer Donley, *Medication Abortion Exceptionalism*, 107 CORNELL L. REV. 627, 634–35 (2022))). Past instances of prosecution have occurred when healthcare professionals report patients they suspect of terminating their pregnancies. *Id.* at 1707.

²³⁰ Conti-Cook, *supra* note 203, at 5, 36 (“If abortion, self-induced abortion, possession of abortion pills, mailing of abortion pills, or assisting an abortion are criminalized across the U.S., there is no reason to believe that prosecutors or police will hesitate to perform forensics analysis on digital devices as part of an investigation into unlawful abortions.”).

²³¹ *Id.* at 3–5.

healthcare team suspected that Ms. Fisher had committed a crime and reported her to law enforcement.²³² In front of the grand jury, prosecutors presented evidence of Ms. Fisher's web history and online purchase of abortion pills.²³³ The grand jury subsequently indicted her for second degree murder.²³⁴

Given the extensive reproductive health data ecosystem, one could easily imagine a zealous prosecutor going beyond merely following potential leads, and instead actively searching for those who have undergone an abortion. For example, Senator Ron Wyden of Oregon and several other members of Congress recently foresaw this possibility when, in May 2022, they wrote to the CEO of Google, urging the company to stop "unnecessarily collecting and retaining customer location data."²³⁵ The letter warned that, if abortion became illegal, "it is inevitable that right-wing prosecutors will obtain legal warrants to hunt down, prosecute and jail women for obtaining critical reproductive health care."²³⁶ Senator Wyden envisioned that prosecutors could obtain a warrant for all cellphones that entered a geofenced area surrounding an abortion clinic,²³⁷ employing the same strategy as the advertisers discussed above.²³⁸

²³² *Id.* at 3–4.

²³³ *Id.* at 4.

²³⁴ *Id.*

²³⁵ Letter from Ron Wyden et al., U.S. Sens., to Sundar Pichai, Chief Exec. Officer, Google LLC 1 (May 24, 2022) (on file with author).

²³⁶ *Id.* at 2. Other members of Congress are continuing to explore these issues. Adam Schwartz, *Congress Probes How Location Data Brokers Threaten Reproductive Privacy*, ELEC. FRONTIER FOUND. (July 12, 2022), <https://www.eff.org/deeplinks/2022/07/congress-probes-how-location-data-brokers-threaten-reproductive-privacy> [<https://perma.cc/E33M-TY7K>].

²³⁷ Letter from Ron Wyden et al. to Sundar Pinchai, *supra* note 235, at 2 (noting that Google received 11,554 geofence warrants from law enforcement in 2020, which shows that it is a common practice in investigations). Further research shows that this use of warrants is most common in states with greater abortion restrictions and those seeking to impose greater abortion restrictions. Alfred Ng, *'A Uniquely Dangerous Tool': How Google's Data Can Help States Track Abortions*, POLITICO (July 18, 2022), <https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906> [<https://perma.cc/33J3-RCFT>]. One report shows that geofence warrants account for more than half of all search warrants in the United States. CAHN & MANIS, *supra* note 26, at 5. It is important to note that even though geofence warrants are currently a widespread practice, they were recently ruled unconstitutional by a U.S. district court. *United States v. Chatrie*, 590 F. Supp. 3d 901, 929–33 (E.D. Va. 2022); *see also* Denise Lavoie, *'Geofence Warrant' Unconstitutional, Judge Rules in Virginia*, AP NEWS (Mar. 30, 2022), <https://apnews.com/article/virginia-robbery-d20d767fa1ef52a8b69e76adb8626837> [<https://perma.cc/3NM8-U35P>]. This case is currently being appealed in the Fourth Circuit. *United States v. Chatrie*, No. 22-04489 (4th Cir. appeal docketed Aug. 29, 2022).

²³⁸ *See supra* Subsection I.B.1. Of course, geofence warrants would not capture information about individuals who terminated their pregnancies via self-managed abortions with medication shipped to their homes. Given the breadth of the reproductive health data ecosystem, however, any number of data points could sweep large numbers of individuals into an investigation, such as information about internet searches for medication abortion, as in the individualized case of Ms. Fisher. Conti-Cook, *supra* note 203, at 3–5; Ben Leonard, *'Uterus Surveillance': The Scramble to Keep Abortion Data from Prying Eyes*, POLITICO (May 20, 2022), <https://politico.com/news/2022/05/20/uterus-surveillance-the-scramble-to-keep-abortion-data-from-prying-eyes-00033775> [<https://perma.cc/NH5M-VD66>] (noting

Law enforcement could use any number of data points for such wide-scale searches. A key example post-*Dobbs* will relate to interstate travel. Many individuals in states with restrictive abortion laws will travel to states where abortion remains legal.²³⁹ This travel will create a digital footprint that ranges from purchasing plane tickets to seeking monetary support from abortion funds to arranging accommodation or childcare for the trip.²⁴⁰

Law enforcement can access this data in several ways. As foreshadowed by Senator Wyden's letter, law enforcement can issue a warrant asking companies to hand over information that meets certain criteria.²⁴¹ Additionally, because our lax privacy laws have created vast monetization of personal data, police can also thwart warrant requirements by simply purchasing individual data from data brokers.²⁴² This practice is widely used outside of the reproduc-

the vast array of data points that could be accessed by law enforcement, including internet searches, interactions with online advertisements for telehealth abortion care, and cookies from abortion providers' websites); see also Conti-Cook, *supra* note 203, at 56 (noting that law enforcement "could potentially subpoena [internet service providers] for the IP addresses of every search for 'abortion medication' or 'abortion pills' or any other keyword combination").

²³⁹ Benjamin Rader et al., *Estimated Travel Time and Spatial Access to Abortion Facilities in the US Before and After the Dobbs v. Jackson Women's Health Decision*, 328 JAMA 2041, 2046 (2022) (noting that, in particular, individuals who are Black, Indigenous, and people of color would experience "large absolute increases in travel time to abortion facilities" and low income individuals would "continue[] to have low access to abortion facilities").

²⁴⁰ In his *Dobbs* concurrence, Justice Brett Kavanaugh wrote that he thought the question of whether one could continue to travel to other states to obtain an abortion was "not especially difficult as a constitutional matter." 142 S. Ct. 2228, 2309 (2022) (Kavanaugh, J., concurring) ("[M]ay a State bar a resident of that State from traveling to another State to obtain an abortion? In my view, the answer is no based on the constitutional right to interstate travel."). Commentators, however, widely acknowledge that the right to interstate travel post-*Dobbs* will be heavily contested. See, e.g., I. Glenn Cohen, Melissa Murray & Lawrence O. Gostin, Opinion, *The End of Roe v. Wade and New Legal Frontiers on the Constitutional Right to Abortion*, 328 JAMA 325, 326 (2022); Cohen et al., *supra* note 130, at 21–23. The lack of data privacy surrounding any travel out of state increases the complexity of these debates and potentially chills behaviors of those seeking to travel out of state or to assist others in traveling out of state.

²⁴¹ Although there needs to be probable cause to issue a warrant, it is not necessarily a difficult barrier for law enforcement to overcome. Jolynn Dellinger & Stephanie Pell, *The Impotence of the Fourth Amendment in a Post-Roe World*, LAWFARE (June 13, 2022), <https://www.lawfareblog.com/impotence-fourth-amendment-post-ro-worl> [<https://perma.cc/JGB2-5RYD>]. For example, in the case of a geofence warrant around an abortion clinic, it is easy to imagine that law enforcement could establish probable cause that those entering the clinic may be undertaking or "aiding and abetting" an abortion.

²⁴² See, e.g., Stephanie Lacambra & Jennifer Lynch, *Senator Wyden Demands Answers from Prison Phone Service Caught Sharing Cellphone Location Data*, ELEC. FRONTIER FOUND. (May 11, 2018), <https://www EFF.org/deep links/2018/05/senator-wyden-calls-fcc-investigate-real-time-location-data-sharing-all-cellphone> [<https://perma.cc/E4FC-DTDD>]; Bennett Cyphers, *How the Federal Government Buys Our Cell Phone Location Data*, ELEC. FRONTIER FOUND. (June 13, 2022), <https://www EFF.org/deep links/2022/06/how-federal-government-buys-our-cell-phone-location-data> [<https://perma.cc/XS5A-VN3E>]. A bipartisan bill, called The Fourth Amendment Is Not for Sale Act, was introduced in Congress to prevent law enforcement from acquiring or purchasing data from data brokers in situa-

tive health context, but is easily transferable. Indeed, in one example, federal immigration officers used purchased data to track menstrual cycles of immigrants and identify pregnant individuals to pressure them, some young teenagers, into continuing the pregnancies and not seeking an abortion.²⁴³

This Article predominately focuses on reproductive health information that exists outside of the medical setting, and, therefore, outside of the bounds of HIPAA protections. But law enforcement can, in certain circumstances, legally access medical records because HIPAA allows sharing for criminal investigations.²⁴⁴ Thus, providers are being encouraged to think carefully about the information that they seek and place into medical records post-*Dobbs*.²⁴⁵ Recent guidance from the U.S. Department of Health and Human Services (HHS) clarified when disclosure to law enforcement was *permitted* without patient authorization versus when it was *required*, arguing that disclosures to law enforcement are “narrowly tailored.”²⁴⁶ The guidance also clarified when providers are prohibited from sharing medical information.²⁴⁷ The guidance indicates that reporting suspected abortions to law enforcement without a specific request for information will often be prohibited since state laws do not generally require such reporting.²⁴⁸

It is important to reinforce that, at this time, it is likely that most law enforcement activity is either targeted toward providers and helpers or comes

tions that would normally require a warrant. The Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. (2021).

²⁴³ Conti-Cook, *supra* note 203, at 55; see also Jennifer Wright, *The U.S. Is Tracking Migrant Girls’ Periods to Stop Them from Getting Abortions*, HARPER’S BAZAAR (Apr. 2, 2019), <https://www.harpersbazaar.com/culture/politics/a26985261/trump-administration-abortion-period-tracking-migrant-women/> [https://perma.cc/S6NP-AQ3N].

²⁴⁴ Carleen M. Zubrzycki, *The Abortion Interoperability Trap*, 132 YALE L.J.F. 197, 218–19 (2022), https://www.yalelawjournal.org/pdf/F7.ZubrzyckiFinalDraftWEB_6jsh8oxp.pdf [https://perma.cc/P4Y9-CDPG]; Eric Boodman, Tara Bannow, Bob Herman & Casey Ross, *HIPAA Won’t Protect You if Prosecutors Want Your Reproductive Health Records*, STAT (June 24, 2022), <https://www.statnews.com/2022/06/24/hipaa-wont-protect-you-if-prosecutors-want-your-reproductive-health-records/> [https://perma.cc/77AJ-8DRW].

²⁴⁵ Spector-Bagdady & Mello, *supra* note 40, at 2 (advising that clinicians “[r]ecording less information may be more protective”).

²⁴⁶ *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, U.S. DEP’T OF HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html> [https://perma.cc/E87E-3GAZ] (June 29, 2022).

²⁴⁷ *Id.*

²⁴⁸ *Id.* (explaining that “[i]n the absence of a mandate enforceable in a court of law, the Privacy Rule’s permission to disclose PHI for law enforcement purposes does not permit a disclosure to law enforcement where a hospital or other health care provider’s workforce member chose to report an individual’s abortion or other reproductive health care,” regardless of “whether the workforce member initiated the disclosure to law enforcement or others or the workforce member disclosed PHI at the request of law enforcement” (internal citation omitted)).

from specific reports, rather than dragnet sweeps of vast data.²⁴⁹ As the Electronic Frontier Foundation (EFF) noted regarding calls to delete Femtech apps:

[I]t's useful to distinguish between the security and privacy threats that abortion seekers are actively experiencing *now* versus threats that may come in the future. Dragnet surveillance of period tracking apps in order to identify people with menstrual irregularities or other supposed evidence of terminated pregnancy fits squarely in the latter category.²⁵⁰

Although dragnet surveillance is currently a future threat, once police begin to investigate an individual, their internet searches, browser history, and text messages all can become important evidence.²⁵¹ As will be discussed, this means that individuals interested in self-managing their abortions may also need to think about self-managing their privacy.²⁵² Additionally, depending on how law enforcement responds to growing abortion restrictions across the states, the current trend to focus on providers, helpers, and specific individuals could morph into broader use of surveillance data. "This new data-driven era . . . does not represent a return to a way of life reminiscent of the 1960s; today's communications technologies and services will enable government surveillance of the details of women's lives to a degree never before seen."²⁵³ It is imperative for policymakers to shore up privacy rights now to prevent these concerns from actualizing.²⁵⁴

2. Impacts Across Reproductive Health and Support Networks

The increased investigation of abortion will impact not only those who are seeking to terminate their pregnancies, but also women experiencing a wide variety of reproductive health needs across the country. A potential counterargument to concerns about how reproductive health data can be leveraged in criminal investigations is that law enforcement should be able to access information that helps them to investigate crimes. If something is illegal, so the

²⁴⁹ See, e.g., Conti-Cook, *supra* note 203, at 58 (noting that, at the time of writing pre-*Dobbs*, government enforcers seeking to limit illegal self-managed abortion focused on the providers of pills, rather than the individuals using them).

²⁵⁰ Gennie Gebhart & Daly Barnett, *Should You Really Delete Your Period Tracking App?*, ELEC. FRONTIER FOUND. (June 30, 2022), <https://www.eff.org/deeplinks/2022/06/should-you-really-delete-your-period-tracking-app> [<https://perma.cc/34Q6-TSYM>].

²⁵¹ *Id.*

²⁵² See *infra* Section IV.A.

²⁵³ Dellinger & Pell, *supra* note 241.

²⁵⁴ See *infra* Section IV.C.

argument goes, law enforcement should be able to investigate to the fullest.²⁵⁵ After all, police and prosecutors utilize personal data in convictions for drug offenses and white-collar crimes—what would the difference be for other newly established reproductive crimes? The answer is that a lack of privacy can affect many more individuals than only those with “incriminating” data and, in the case of reproductive health in particular, there are not crisp lines between abortion, access to birth control, and necessary medical care during pregnancy and pregnancy loss. Thus, loss of privacy and increased penalization for one aspect of reproductive healthcare naturally implicates all of reproductive health.

For example, not all pregnancy outcomes that look like abortion will be illegal, even in states with highly restrictive laws. Yet, a lack of privacy regarding pregnancy outcomes could lead to investigations and harassment targeting someone experiencing loss. “Self-managed abortion mimics the experience of pregnancy loss, making it difficult for states to enforce strict abortion laws without further investigating and criminalizing miscarriage and stillbirth.”²⁵⁶ Additionally, even someone who has contemplated pregnancy termination may experience pregnancy loss, given the high rates of miscarriage.²⁵⁷ Assuming this person has some personal data, such as internet searches or text messages, indicating that they were considering termination, this could open them up to increased investigation and even prosecution despite no illegal act occurring. “Neither abortion nor pregnancy loss patients deserve this scrutiny.”²⁵⁸ Increased investigations will chill behavior and harm those experiencing all pregnancy outcomes, not only abortion.²⁵⁹

Additionally, with growing abortion restrictions, law enforcement foreseeably could be interested in a wide array of actions taken during pregnancy if women are seen as placing their unborn children in harm’s way.²⁶⁰ This would

²⁵⁵ This argument parallels the perennial privacy argument that privacy violations may not be of large concern because an individual feels that they have nothing to hide. *See generally* Daniel J. Solove, “*I’ve Got Nothing to Hide*” and Other Misunderstandings of Privacy, 44 SAN DIEGO L. REV. 745 (2007) (discussing how many do not view privacy violations as intrusions if nothing illegal is identified, but when something illegal is identified, there are arguments that there was not a legitimate justification for privacy for the illegal activity). Professor Solove ultimately argues that the “nothing to hide” framework incorrectly frames privacy. *Id.* at 764. “[T]he problem with the nothing to hide argument is the underlying assumption that privacy is about hiding bad things. Agreeing with this assumption concedes far too much ground and leads to an unproductive discussion of information people would likely want or not want to hide.” *Id.*

²⁵⁶ Donley & Lens, *supra* note 1, at 1704.

²⁵⁷ Conti-Cook, *supra* note 203, at 51 (noting that “it is not uncommon for a woman contemplating an abortion to coincidentally suffer a miscarriage”).

²⁵⁸ Donley & Lens, *supra* note 1, at 1711.

²⁵⁹ *Id.*

²⁶⁰ PREGNANCY JUST., *supra* note 118, at 9 (noting that prosecutors have brought various kinds of cases against pregnant individuals, including for failing to wear a seatbelt while pregnant).

bring even greater focus on the behaviors of pregnant individuals.²⁶¹ One can imagine the vast array of data that could be paired with reproductive health data to infer that a woman may be “harming” her unborn child. “Any number of ‘bad behaviors’ by pregnant people could . . . be surveilled with a range of available technology.”²⁶² Drug and alcohol use has already often been targeted by law enforcement,²⁶³ and this could easily expand to other decisions that could be digitally surveilled, such as decisions about whether or not to medicate.²⁶⁴ Taken to the extreme, a wide variety of activities that are not recommended for pregnant women could come under suspicion, from eating raw fish, to drinking too much coffee, to cleaning out a cat’s litter box.²⁶⁵ Broad reproductive health data surveillance will make it easy for those who are interested to track the actions of pregnant individuals, from conception to birth.

As investigations and prosecutions of pregnant individuals will likely continue to grow post-*Dobbs*, law enforcement will also continue to focus on those “aiding and abetting” access to abortion. For example, model legislation proposed by the National Right to Life Committee recommends increasing penalties for those helping individuals gain access to abortions.²⁶⁶ Abortion networks today have a wide variety of information online.²⁶⁷ This allows for broader access to information about safe abortions and support networks, but also leaves digital trails to the whole network of abortion supporters, friends, and family.²⁶⁸ In states with severe restrictions, the enormous amount of data available to law enforcement could place those assisting individuals in access-

²⁶¹ Indeed, increased law enforcement investigation can implicate all those able to get pregnant. For example, a woman in Alabama was recently jailed for drug use because of the harm it could cause to her unborn child despite the fact that she was not currently pregnant. Amy Yurkanin, *Alabama Woman Jailed for Using Drugs During Pregnancy Wasn’t Pregnant, Lawsuit Says*, AL.COM (Nov. 20, 2022), <https://www.al.com/news/2022/11/alabama-woman-jailed-for-using-drugs-during-pregnancy-wasnt-pregnant-lawsuit-says.html> [<https://perma.cc/5NN5-FW5C>].

²⁶² Conti-Cook, *supra* note 203, at 7–8 (quoting Kira Proehl, Comment, *Pregnancy Crimes: New Worries to Expect When You’re Expecting*, 53 SANTA CLARA L. REV. 661, 682 (2013)). Beyond surveillance by technology, even disclosing this information to healthcare providers could be problematic if state mandatory reporting laws are interpreted broadly to cover abortion and harm during pregnancy, particularly with life being defined at fertilization. Spector-Bagdady & Mello, *supra* note 40, at 2.

²⁶³ See generally PREGNANCY JUST., *supra* note 118 (discussing the prosecution of individuals for substance use while pregnant).

²⁶⁴ Conti-Cook, *supra* note 203, at 6.

²⁶⁵ *Id.* at 8–9.

²⁶⁶ Memorandum from James Bopp, Jr., NRLC Gen. Couns., Courtney Turner Milbank & Joseph D. Maughon to the Nat’l Right to Life Comm. 5–6 (June 15, 2022) (on file with author).

²⁶⁷ Conti-Cook, *supra* note 203, at 10 (asking readers to “[i]magine what Jane—the underground abortion network that grew out of Chicago in the pre-*Roe* late sixties—would look like today if abortions were criminalized,” and remarking that “[i]nstead of hanging flyers on campuses and putting advertisements in newspapers . . . in today’s world, there may be Instagram accounts, websites, email addresses, and a Facebook group”).

²⁶⁸ *Id.* at 10–11.

ing abortions in legal jeopardy as well.²⁶⁹ In a recent example, prosecutors in Nebraska gained access to Facebook messages directly from Facebook itself, and used messages between a mother and her daughter to collect further data and to press charges for terminating a pregnancy.²⁷⁰

Overall, it is clear that the vast reproductive health data ecosystem allows law enforcement easy access to sensitive health information of individuals and their support networks. Yet, police are not the only actors potentially interested in accessing this ecosystem for use in ways that could be harmful to women and pregnant individuals.

B. Citizen Access to Reproductive Health Data

Even without the power of warrants, it is easy for other individuals and groups to purchase data, like law enforcement has done. Scores of data brokers sell information about pregnancy and reproductive health for pennies on the dollar.²⁷¹ Sometimes, entities may access this data for potentially beneficial reasons, such as research.²⁷² Other times, the data could be accessed by anti-abortion groups or everyday citizens interested in limiting abortions or penalizing those who decide to terminate their pregnancies.²⁷³

²⁶⁹ Blake Farmer, *Self-Managed Abortions Gain Attention, but Helpers Risk Legal Trouble*, KAI-SER HEALTH NEWS (July 12, 2022), <https://khn.org/news/article/self-managed-abortions-risk-legal-trouble/> [<https://perma.cc/CM2L-E4N9>]; see also Surana, *supra* note 220 (noting that anti-abortion activists in Tennessee are encouraging mining of health data to target doctors who are performing abortions).

²⁷⁰ Jason Koebler & Anna Merlan, *This Is the Data Facebook Gave Police to Prosecute a Teenager for Abortion*, VICE (Aug. 9, 2022), <https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion> [<https://perma.cc/PB77-C775>]. They were charged with concealing a death and improper disposal of human remains, and the mother was also charged with performing an abortion because she purchased abortion medication for her daughter. Kaste, *supra* note 68.

²⁷¹ Shoshana Wodinsky & Kyle Barr, *These Companies Know When You're Pregnant—and They're Not Keeping It Secret*, GIZMODO (July 30, 2022), <https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426> [<https://perma.cc/24FD-KUAM>] (noting that data about a user's pregnancy status can be purchased cheaply—approximately 50¢ to \$2).

²⁷² Indeed, underreporting of pregnancy outcomes, such as abortion, impact the quality of pregnancy research overall, highlighting the importance of robust data access for researchers. Sheila Desai, Laura D. Lindberg, Isaac Maddow-Zimet & Kathryn Kost, *The Impact of Abortion Underreporting on Pregnancy Data and Related Research*, 25 MATERNAL & CHILD HEALTH J. 1187, 1190 (2021). Another example of researcher use of the reproductive data ecosystem is studies that show an uptick of Google searches for abortion medications following abortion restrictions in states. See, e.g., Conti-Cook, *supra* note 203, at 26–27 (using Google Trends to analyze the frequency of searches for “abortion pills” across states compared to the states with the most abortion restrictions); Poliak et al., *supra* note 175, at 1003 & fig. (exploring internet search trends regarding abortion medications after the leaked *Dobbs* decision).

²⁷³ Mahdawi, *supra* note 14.

For example, those interested in limiting abortions have used personal data to persuade individuals not to undergo abortions through misinformation and harassment.²⁷⁴ Historically, anti-abortion activists collected license plate numbers of cars traveling to abortion clinics to match the plates with identities and harass the patients in the future.²⁷⁵ As discussed above, one group even utilized geofencing to send targeted advertisements to “abortion-minded women” to try to dissuade them from undergoing the procedure.²⁷⁶ Anti-abortion groups have even developed their own Femtech period-tracking app that is deceptively designed to persuade users not to terminate pregnancies.²⁷⁷ Similarly, abortion advocates worry that crisis pregnancy centers—which look like health clinics, but seek to dissuade pregnant individuals from getting abortions—will collect copious amounts of data²⁷⁸ and provide law enforcement with information about who may be seeking to terminate a pregnancy.²⁷⁹

Post-*Dobbs*, private groups and individuals will likely continue to gather private, intimate reproductive health data. This will be especially true in states that adopt laws modeled after Texas’s Senate Bill 8 (S.B. 8) and the new strategy of creating a vigilante system to enforce abortion penalties. In the fall of

²⁷⁴ CAHN & MANIS, *supra* note 26, at 2–3.

²⁷⁵ Anna Quindlen, Opinion, *Public & Private; At the Clinics*, N.Y. TIMES, Apr. 5, 1992, at E17 (noting that patients of an abortion clinic were mailed pictures of bloody fetuses after their license plates were traced at an appointment); Jacqueline Darroch Forrest & Stanley K. Henshaw, *The Harassment of U.S. Abortion Providers*, 19 FAM. PLAN. PERSPS. 9, 10 (1987) (finding that 16% of abortion facilities surveyed reported that patients were called or visited at home following an appointment after their license plate was traced); Alice Clapman, Note, *Privacy Rights and Abortion Outing: A Proposal for Using Common-Law Torts to Protect Abortion Patients and Staff*, 112 YALE L.J. 1545, 1546 (2003).

²⁷⁶ See Prince, *supra* note 47, at 65 (quoting Press Release, *supra* note 75); *supra* Subsection I.B.1.

²⁷⁷ Citron, *A New Compact*, *supra* note 14, at 1803–04 (noting that the app fails to disclose to users its motivation and provides misleading information, such as about the safety of birth control, despite claiming to provide users with “cutting edge science” (quoting *FEMM Health Period and Ovulation Tracker*, GOOGLE PLAY, <https://play.google.com/store/apps/details?id=org.femmhealth.femm&hl=en+US&pli=1> [<https://perma.cc/BFT8-57AH>])).

²⁷⁸ *How Anti-Abortion Activism Is Exploiting Data*, PRIV. INT’L (July 22, 2019), <https://privacyinternational.org/long-read/3096/how-anti-abortion-activism-exploiting-data> [<https://perma.cc/9KVV-FQM8>]; Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-abortion Clinics Are Collecting Highly Sensitive Info 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/4QV5-Q6C4>].

²⁷⁹ Abigail Abrams & Vera Bergengruen, *Anti-abortion Pregnancy Centers Are Collecting Troves of Data That Could Be Weaponized Against Women*, TIME (June 22, 2022), <https://time.com/6189528/anti-abortion-pregnancy-centers-collect-data-investigation/> [<https://perma.cc/9A69-8BLS>]; Press Release, Michael Bennet, Sen., U.S. Senate, Bennet, Cortez Masto Call on HHS to Update HIPAA Privacy Rule to Protect Reproductive Rights (July 1, 2022), <https://www.bennet.senate.gov/public/index.cfm/2022/7/bennet-cortez-masto-call-on-hhs-to-update-hipaa-privacy-rule-to-protect-reproductive-rights> [<https://perma.cc/WL5R-4VPP>].

2021, a full nine months before *Roe* was overturned, the Texas State Legislature passed S.B. 8, a now infamous law that effectively halted abortions in the state six weeks beyond a woman's last menstrual cycle.²⁸⁰ S.B. 8 thwarted successful constitutional challenges by placing the law's enforcement power in the hands of everyday citizens, not the state.²⁸¹

To the extent that S.B. 8 is modeled in other states, there will be an increase in the number of groups and individuals interested in gathering data about abortions.²⁸² Indeed, because the bounty system of S.B. 8 relies on civil enforcement rather than criminal enforcement, it is an attractive model for anti-abortion activists targeting interstate travel for abortions.²⁸³ For example, one anti-abortion group in Texas proposed a bill that would employ the S.B. 8 model to target anyone who pays for an individual to receive an out-of-state abortion.²⁸⁴

So far, S.B. 8 follows the framework common in criminal law—to only penalize those who provide or support abortion, rather than the individual undertaking the abortion themselves.²⁸⁵ Thus, for now, S.B. 8 and similarly mod-

²⁸⁰ S.B. 8, 87th Leg. (Tex. 2021) (codified at TEX. HEALTH & SAFETY CODE ANN. § 171.208 (West 2021)).

²⁸¹ TEX. HEALTH & SAFETY CODE ANN. § 171.208(a) (empowering “[a]ny person, other than an officer or employee of a state or local governmental entity in this state” to bring a civil action enforcing the law).

²⁸² See Yvonne Lindgren, *Dobbs v. Jackson Women’s Health and the Post-Roe Landscape*, 35 J. AM. ACAD. MATRIM. LAWS. 235, 274–75 (2022). Laws modeled after S.B. 8 have already been proposed in other states. See, e.g., Caroline Kitchener, *Missouri Lawmaker Seeks to Stop Residents from Obtaining Abortions Out of State*, WASH. POST (Mar. 8, 2022), <https://www.washingtonpost.com/politics/2022/03/08/missouri-abortion-ban-texas-supreme-court/> [<https://perma.cc/48GZ-MXJ8>]; CAHN & MANIS, *supra* note 26, at 7. A recently passed statute in Oklahoma includes a similar enforcement mechanism. S.B. 1503, 58th Leg., Reg. Sess. (Okla. 2022).

²⁸³ Emma Bowman, *As States Ban Abortion, the Texas Bounty Law Offers a Way to Survive Legal Challenges*, NPR (July 11, 2022), <https://www.npr.org/2022/07/11/1107741175/texas-abortion-bounty-law> [<https://perma.cc/S6KZ-J9TF>].

²⁸⁴ Becky Sullivan, *Texas Conservatives Have a Plan to Get Around DAs Who Won’t Enforce Abortion Laws*, NPR (July 15, 2022), <https://www.npr.org/2022/07/15/1111383520/texas-abortion-laws-prosecutors> [<https://perma.cc/WS7J-PTZ4>].

²⁸⁵ The law is incredibly broad in the scope of who can be sued, from providers to individuals who “aid and abet” the performance of an abortion by a licensed Texas provider. TEX. HEALTH & SAFETY CODE ANN. § 171.208(a)(1), (2). The aiding and abetting clause includes individuals “regardless of whether the person knew or should have known that the abortion would be performed or induced,” causing speculation that even a ride-share driver taking an individual to an appointment could be at risk of a hefty civil fine. *Id.* § 171.208(a)(2); *Lyft, Uber Will Pay Drivers’ Legal Fees if They’re Sued Under Texas Abortion Law*, NPR (Sept. 8, 2021), <https://www.npr.org/2021/09/08/1035045952/lyft-uber-will-pay-drivers-legal-fees-if-theyre-sued-under-texas-abortion-law> [<https://perma.cc/97KH-8WTP>]. Yet, despite the breadth of the law, S.B. 8 specifically states that it does not “authorize the initiation of a cause of action against or the prosecution of a woman on whom an abortion is performed or induced” TEX. HEALTH & SAFETY CODE ANN. § 171.206(b)(1). In a well-publicized case, a woman in Texas was arrested for murder in 2022 after being accused of self-inducing an abortion, notwithstanding the fact that both Texas’s criminal fetal homicide law and S.B. 8 explicitly ex-

eled laws will predominately focus on those supporting abortion. Nevertheless, given the complexities of regulating both self-managed abortion and access to abortion across state lines, there may be efforts in the future to expand the S.B. 8 model to pregnant people themselves.²⁸⁶ Either way, the reproductive health data ecosystem will provide ample information regarding the activities of both pregnant women and their support and healthcare networks.

C. Third-Party Access and Discrimination

Advertisers, law enforcement, and citizens are not the only end users for the treasure trove of data that companies amass. Reproductive health information could also end up in the hands of other third parties, such as insurers and employers. This increases the risk of discrimination based on reproductive health information. Pregnancy status and outcomes have historically led to discrimination and stigmatization. Especially in the workplace, pregnant individuals can face dismissal, negative comments about their physical appearance, and other forms of discrimination.²⁸⁷ These harms continue to exist despite the Pregnancy Discrimination Act (PDA)²⁸⁸ and, paralleling the prosecution of pregnancy status, the harms disproportionately fall on marginalized communities.²⁸⁹

In some instances, individuals are likely aware that their data may be shared with third parties, such as employers. Consider Ovia, a Femtech pregnancy-tracking app that has partnered with employers and incentivizes employees to use the app as part of workplace wellness programs.²⁹⁰ The employers then get aggregated information telling them about the number of pregnan-

cluded the pregnant individual from its ambit. The case was eventually dismissed, but it highlights that any amount of criminalization of abortion will likely increase investigations of women. Pablo de la Rosa, Carolina Cuellar, Dan Katz & Fernando Ortiz Jr., *DA Moves to Dismiss a Murder Charge Against a Texas Woman Accused of Self-Induced Abortion*, HOUS. PUB. MEDIA (Apr. 9, 2022), <https://www.houstonpublicmedia.org/articles/news/criminal-justice/2022/04/09/423004/texas-woman-charged-with-murder-for-self-induced-abortion/> [<https://perma.cc/CJ2A-UZP4>].

²⁸⁶ Even if these types of laws are not directed at individuals undergoing an abortion, they will still increase surveillance of pregnant people generally. Lindgren, *supra* note 282, at 275.

²⁸⁷ Deborah L. Brake & Joanna L. Grossman, *Unprotected Sex: The Pregnancy Discrimination Act at 35*, 21 DUKE J. GENDER L. & POL'Y 67, 68 (2013); Natalie Kitroeff & Jessica Silver-Greenberg, *Pregnancy Discrimination Is Rampant Inside America's Biggest Companies*, N.Y. TIMES (Feb. 8, 2019), <https://www.nytimes.com/interactive/2018/06/15/business/pregnancy-discrimination.html> [<https://perma.cc/8XF6-J7U2>].

²⁸⁸ The Pregnancy Discrimination Act of 1978, 42 U.S.C. § 2000e(k). Congress enacted the Pregnancy Discrimination Act (PDA) of 1978, Pub. L. No. 95-555, 92 Stat. 2076 (codified at 42 U.S.C. § 2000e), to respond to employment harms experienced by pregnant individuals, often grounded in social stereotypes of gender and maternal norms. See Brake & Grossman, *supra* note 287, at 71–77.

²⁸⁹ Brake & Grossman, *supra* note 287, at 69.

²⁹⁰ Harwell, *supra* note 16.

cies among employees, plans to return to work after the birth of a child, pregnancy losses, and searches conducted on the app.²⁹¹ One of the stated benefits of the program is to help employers facilitate women's reentry back into the workplace more quickly after childbirth.²⁹² Although the information given to the employer is de-identified, aggregated information, it may not be difficult in some small workplaces to identify pregnant individuals.²⁹³

When employers and insurers get access to reproductive health information, it could lead to increased premiums or minimized benefits offered in a certain plan.²⁹⁴ This is a common concern of workplace wellness programs in general,²⁹⁵ but given how closely pregnancy is linked with time away from work and potential increases in employer health costs, employer tracking of reproductive health is of particular concern.

Additionally, the trove of data regarding reproductive health could be used in algorithms that screen potential employees in ways that are discriminatory.²⁹⁶ This is especially concerning if data that can be used to infer pregnancy is used by algorithms as proxies.²⁹⁷ Data that reveals information about pregnancy, or even data that suggests a possible future pregnancy, could lead to problematic, discriminatory results in the hands of algorithms.²⁹⁸ Similar risks could arise if the data is collected by lenders or insurers.²⁹⁹ Current laws, such as the PDA, do little to prevent this problematic type of proxy discrimination.³⁰⁰ In fact, unless there is greater oversight of algorithmic decisions, such discrimination is inevitable.³⁰¹ The reproductive health data ecosystem only further entrenches this inevitability.

²⁹¹ *Id.*

²⁹² *Id.*

²⁹³ *Id.*; Stephanie R. Morain, Leah R. Fowler & Jessica L. Roberts, Opinion, *What to Expect When [Your Employer Suspects] You're Expecting*, 176 JAMA INTERNAL MED. 1597, 1597 (2016).

²⁹⁴ Harwell, *supra* note 16; Marshall Allen, *Health Insurers Are Vacuuming Up Details About You—and It Could Raise Your Rates*, PROPUBLICA (July 17, 2018), <https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates> [https://perma.cc/LA4B-KNLL].

²⁹⁵ Jill R. Horwitz, Brenna D. Kelly & John E. DiNardo, *Wellness Incentives in the Workplace: Cost Savings Through Cost Shifting to Unhealthy Workers*, 32 HEALTH AFFS. 468, 474 (2013).

²⁹⁶ Gilman, *supra* note 11, at 105.

²⁹⁷ See Prince & Schwarcz, *supra* note 71, at 1273–76 (arguing that if a protected trait is predictive of outcomes, such as likelihood to take time off work, an algorithm will inevitably find proxy information to discriminate on this basis without protective measures being taken).

²⁹⁸ *Id.* at 1286–88.

²⁹⁹ Gilman, *supra* note 11, at 105 (arguing that data from Femtech apps could result in higher insurance or loan rates).

³⁰⁰ Prince & Schwarcz, *supra* note 71, at 1283–84, 1286–87.

³⁰¹ *Id.* at 1263.

IV. PROTECTING REPRODUCTIVE HEALTH PRIVACY

Given the extensive collection of reproductive health data, the widespread ability to access this data by law enforcement, civilians, and other entities, and the grave consequences that stem from this potential access, there is an imperative need for greater protection of reproductive health privacy. Wide access to this data creates a surveillance state that chills behavior and speech in ways that will harm broader reproductive rights.³⁰²

In the short time since the U.S. Supreme Court's 2022 *Dobbs v. Jackson Women's Health Organization* decision, there have been countless examples of how the lack of privacy surrounding reproductive health has had a chilling effect. Women have been encouraged to delete their Femtech apps.³⁰³ Physicians have been implored to think differently about what they report in medical records.³⁰⁴ And there are concerns that restrictions in some states will thwart the free flow of information about reproductive choices in other states where it is legal.³⁰⁵ These changes in behavior may have the effect of insulating some individuals from prosecution for undertaking an abortion or supporting an abortion, but they also will likely affect the ability of thousands of women to fully engage in safe reproductive health choices, including tracking their menstruation, accessing legal abortion, and ensuring healthy pregnancy outcomes.

Of course, a key solution to the harms would be to prevent reproductive health discrimination and to ensure the legality and accessibility of reproductive health choices across the board, including abortion. But, if anything, we are moving toward greater stigmatization, discrimination, and criminalization of reproductive health, thus further necessitating a radical reimaging of how we view data privacy, especially reproductive health data privacy in the United States.

This Part discusses how reproductive health privacy can be strengthened by individual efforts,³⁰⁶ changes in company policies,³⁰⁷ and government action.³⁰⁸ Individual and company efforts on their own can limit the amount of information that flows into the reproductive healthcare data ecosystem, but they cannot fully fix the system. Instead, comprehensive legislation is needed.

³⁰² Solove, *supra* note 255, at 765 (noting that surveillance can chill even legal activity).

³⁰³ Gebhart & Barnett, *supra* note 250.

³⁰⁴ Spector-Bagdady & Mello, *supra* note 40, at 2 (suggesting that “[c]linicians also should not presume that more clinical documentation is always better for managing medicolegal risk”).

³⁰⁵ See Ron Wyden, *The End of Roe and the Threat to Free Speech Online*, SLATE (June 15, 2022), <https://slate.com/technology/2022/06/roe-supreme-court-online-privacy-speech-wyden.html> [<https://perma.cc/5AJ8-HV23>] (arguing that “[s]tep two” of the anti-abortion playbook is to completely stop anyone from talking about abortion online).

³⁰⁶ See *infra* Section IV.A.

³⁰⁷ See *infra* Section IV.B.

³⁰⁸ See *infra* Section IV.C.

A. Privacy Self-Management

The wave of articles encouraging individuals to delete their period tracking apps following the *Dobbs* decision is just one example of privacy self-management—the phenomenon of individuals taking steps to proactively manage what personal data is collected or shared.³⁰⁹ Indeed, privacy self-management is a necessary step in the current U.S. privacy regime. As discussed above, HIPAA, the primary federal law regulating health privacy, does not actually protect the vast amount of reproductive health data that exists outside the healthcare setting.³¹⁰ And although some states are beginning to pass general privacy laws,³¹¹ there is, to date, no comprehensive federal privacy law. Instead, U.S. privacy generally relies on notice and consent—where companies provide individuals with information about the personal data that can be collected and how it may be used, and consumers choose to consent to this collection.³¹² Thus, it is up to individuals to navigate complex privacy notices and decide for themselves what to share, when, and with whom.³¹³ Privacy self-management in general can be difficult,³¹⁴ but especially so in the context of reproductive health.³¹⁵

1. The Difficulties of Privacy Self-Management

Truly protecting one's reproductive health privacy through self-management, however, is a herculean, if not impossible, task.³¹⁶ For starters, agreeing to the privacy policies is often necessary to continue utilizing a good or service. Thus, if an individual needs access to a service, such as a map ap-

³⁰⁹ For a general discussion of privacy self-management and the challenges of this framework, see generally Solove, *supra* note 69.

³¹⁰ See *supra* Section I.C.

³¹¹ Anokhy Desai, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS., <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> [<https://perma.cc/EQW4-ULXJ>] (Apr. 28, 2023).

³¹² See, e.g., Gilman, *supra* note 11, at 109; Solove, *supra* note 69, at 1883–84 (noting that sometimes customers are given a choice to opt out of various aspects of data collection).

³¹³ See, e.g., Solove, *supra* note 102, at 5 (arguing that current privacy regulation depends “too heavily” on individuals self-managing their privacy).

³¹⁴ See *infra* Subsection IV.A.1.

³¹⁵ See *infra* Subsection IV.A.2.

³¹⁶ See, e.g., Prince, *supra* note 105 (showing that even extreme efforts to hide pregnancy status from advertisers can fail); Gilman, *supra* note 11, at 109–10 (explaining that the notice and consent approach fails to protect consumers); Solove, *supra* note 102, at 5 (noting that “[m]anaging one’s privacy is a vast, complex, and never-ending project that does not scale; it becomes virtually impossible to do comprehensively”).

plication to find the location of her doctor's office, she will need to consent to the company's policies.³¹⁷

Additionally, the privacy notices from companies are complex and difficult to read. One study estimates that it would take individuals over eight solid days—201 hours—per year to read every privacy notification.³¹⁸ Moreover, company privacy policies are not static; they can be changed at any time.³¹⁹ If a company decides that it would like to expand the amount of data collected from its users, it simply needs to update its privacy policy to reflect this change.³²⁰ Other than threats to company image and customer trust, there are few barriers preventing companies from pulling the rug out from under customers and significantly changing data practices. Thus, consumers need to continuously monitor potential changes in privacy policies to truly understand how their data is being collected and shared. It is no wonder that most people fail to read the policies and therefore often misunderstand data sharing, often assuming that there is greater privacy protection than there actually is.³²¹

Furthermore, it is not always the individual who controls what data about them are being collected. For example, Senators Elizabeth Warren and Ed Markey recently raised alarm bells about how school surveillance technologies used to monitor student's online activities could end up amassing data about the reproductive health of teens.³²² A letter they wrote to student surveillance platforms reads, in part:

³¹⁷ Citron, *A New Compact*, *supra* note 14, at 1767 (noting that there are not many options, short of simply not using the service, for individuals who do not want to undertake certain privacy risks); *see also* Solove, *supra* note 102, at 37 (noting that “[p]eople who want to fully protect their privacy must forgo using new products, which are increasingly made with internet connections,” as well as “forgo buying things online, using smart phones, paying with credit cards, and using other basic tools of modern life”).

³¹⁸ Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y INFO. SOC'Y 543, 565 (2008).

³¹⁹ *See, e.g.*, Gilman, *supra* note 11, at 110; Jessica L. Roberts & Jim Hawkins, *When Health Tech Companies Change Their Terms of Service*, 367 SCIENCE 745, 745 (2020).

³²⁰ Solove, *supra* note 69, at 1889 (noting that companies frequently make changes to their privacy policies).

³²¹ *See, e.g., id.* at 1886 (citing a study that found that 75% of individuals incorrectly believed that the presence of a privacy policy on a website meant that the company would not share personal data); Fowler & Morain, *supra* note 13, at 212 (noting that privacy policies are often not read and difficult to understand).

³²² Letter from Elizabeth Warren & Edward J. Market, U.S. Sens., to Brian Bason, Chief Exec. Officer, Bark Techs., Inc. 1–2 (July 20, 2022) (on file with author) (informing the CEO of a school surveillance technology company about the concern that these technologies could be used to identify teens seeking information about birth control, abortion, and pregnancy services). For a discussion of student privacy more broadly, *see generally* Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPS*, 8 DREXEL L. REV. 339 (2016) (online corrected) (discussing the limitations of existing student privacy laws given technology and infrastructure innovations).

[P]arents, and students themselves, are often unaware that school districts use monitoring software, or the privacy risks and potential harm associated with these products. It would be deeply disturbing if your software flags words or activity that suggest students are searching for contraception, abortion, or other related services, and if school administrators, parents, and even law enforcement were potentially informed of this activity.³²³

Thus, in some instances, individuals may not even be aware of the types of monitoring they are under, making it even more difficult to self-manage privacy.

All of this makes it incredibly difficult for an individual to limit and manage their private information in the ways they desire. Even if one managed to prevent any company from directly gaining access to information about reproductive health status, this would not address the problem of aggregation—where companies use algorithms to combine “innocuous piece[s] of data” together and infer an intimate fact.³²⁴ When individuals do not even know or comprehend which aspects of their personal data may be used to infer their health statuses, it becomes extremely difficult to limit unwanted sharing of private medical information.³²⁵

2. Reproductive Health Privacy Self-Management Case Study

To understand how difficult privacy self-management would be, it is helpful to brainstorm the steps that one would have to take to limit data collection about reproductive health—say, pregnancy status.³²⁶ Keeping details about a pregnancy private may be important to insulate individuals from targeted ads, especially when there is still a high risk of pregnancy loss, and because knowing that someone is pregnant could potentially open them up to investigation about pregnancy outcomes and behaviors during pregnancy.³²⁷

First, individuals would need to avoid directly sharing with a company that they are pregnant.³²⁸ This would mean opting out of various activities, such as Femtech apps³²⁹ or digitized pregnancy tests.³³⁰ Deleting Femtech apps

³²³ Letter from Warren & Markey to Bason, *supra* note 322, at 2 (footnote omitted).

³²⁴ Solove, *supra* note 69, at 1889–91 (explaining that many privacy harms stem from aggregation).

³²⁵ Solow-Niederman, *supra* note 71, at 361.

³²⁶ This Subsection is by no means meant to be a comprehensive guide to managing privacy. Rather, it illustrates the lengths one would have to go to even begin to try to limit access to data about reproductive health. It is based, in part, on my ultimately unsuccessful attempts to limit advertiser knowledge of my reproductive health status. Prince, *supra* note 105.

³²⁷ See *supra* Section II.B.

³²⁸ See *supra* Subsection I.A.1.

³²⁹ See *supra* Subsection I.A.1.

was likely one of the most common suggestions that surfaced following the *Dobbs* decision.³³¹ But this precaution is only the tip of an incredibly massive iceberg.³³² Companies can learn direct information about reproductive health in other ways. For example, the individual would have to avoid joining any social media support groups,³³³ posting information about pregnancy on social media,³³⁴ or, indeed, sending social media messages or unencrypted texts to family and friends about the pregnancy.³³⁵

Beyond direct information about pregnancy status, the individual would also need to avoid providing information that could be used to infer health status.³³⁶ For example, a big area of concern would be purchases of any pregnancy- or baby-related products, such as prenatal vitamins, pregnancy tests, or maternity clothes. These goods would have to be purchased without using online shopping, credit cards, or loyalty programs.³³⁷ This may be relatively

³³⁰ Frida Garza, *An Internet-Connected Pregnancy Test Comes with Cat Videos and Cooking Tips*, QUARTZ (Apr. 27, 2016), <https://qz.com/670581/an-internet-connected-pregnancy-test-comes-with-cat-videos-and-cooking-tips/> [<https://perma.cc/2XV9-5UKC>].

³³¹ Although this was a common refrain on social media, in reality, the top period-tracking apps increased in downloads following the *Dobbs* decision, suggesting that “users aren’t abandoning their period-tracking apps so much as trading them in for new ones.” Kristen Poli, *The Most Popular Period-Tracking Apps, Ranked by Data Privacy*, WIRED (July 20, 2022), <https://www.wired.com/story/period-tracking-apps-flo-clue-stardust-ranked-data-privacy/> [<https://perma.cc/6JVG-Q97U>].

³³² Kashmir Hill, *Deleting Your Period Tracker Won’t Protect You*, N.Y. TIMES, <https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html> [<https://perma.cc/YTP6-KVAP>] (July 11, 2022); Gebhart & Barnett, *supra* note 250.

³³³ See, e.g., Ostherr & Trotter, *supra* note 57 (detailing the FTC’s settlement with Facebook and highlighting the fact that health information is not protected by the terms of the settlement).

³³⁴ Nora McDonald, *Online Data Could Be Used Against People Seeking Abortions Now That Roe v. Wade Has Been Overturned*, THE CONVERSATION, <https://theconversation.com/online-data-could-be-used-against-people-seeking-abortions-now-that-roe-v-wade-has-been-overturned-182830> [<https://perma.cc/GHH6-EA5Y>] (June 24, 2022).

³³⁵ Janet Vertesi, Opinion, *My Experiment Opting Out of Big Data Made Me Look Like a Criminal*, TIME (May 1, 2014), <https://time.com/83200/privacy-internet-big-data-opt-out/> [<https://perma.cc/8WHF-3CQN>]. Especially post-*Dobbs*, many websites are suggesting that individuals utilize encrypted messaging services, such as Signal, to communicate. Sam Sabin, *Texas Abortion Lawsuit Revives Calls for Encrypted Messaging*, AXIOS (Mar. 14, 2023), <https://www.axios.com/2023/03/14/encrypted-messaging-texas-abortion-suit> [<https://perma.cc/ZEA8-97KY>]. Although this would prevent companies from reading the messages, it does not stop law enforcement from seeing the messages if they gain access to one of the phones on which an encrypted message is stored. See *id.* Similarly, simply deleting a text message sent via unencrypted mechanisms will not necessarily insulate this information from law enforcement. Dustin Jones, *When It Comes to Data on Your Phone, Deleting a Text Isn’t the End of the Story*, NPR (July 15, 2022), <https://www.npr.org/2022/07/15/1111778878/secret-service-deleted-messages-january-6-is-that-data-really-gone> [<https://perma.cc/L3VE-VWJT>].

³³⁶ See *supra* Subsection I.A.2.

³³⁷ Jon Keegan, *Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You*, THE MARKUP (Feb. 16, 2023), <https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you> [<https://perma.cc/K3XP-G59Q>]; CAHN & MANIS, *supra* note 26, at 4 (“When purchasers pay with a credit card, an online account, or with an in-store loyalty card, everyday purchases—medication, pregnancy tests, prenatal vitamins, menstrual prod-

easy for some to implement for small purchases, such as prenatal vitamins, but when dealing with ever larger purchases, such as cribs and strollers, it can appear downright criminal.³³⁸ It also assumes that one lives in an area with access to stores selling a wide variety of needed goods and has the ability to get cash on hand for any necessary purchases.

Although goods can theoretically be purchased in person and with cash, it is a bit harder to access necessary information without going online.³³⁹ Imagine the host of details one may need to learn after becoming pregnant, such as directions to a doctor's office, information about medical questions, and reviews of the best products.³⁴⁰ Accessing this information all in an analog world is extremely time consuming at best. But searching for information online provides companies like Google with a mind-numbing array of information that can point to reproductive health status.³⁴¹ Therefore, someone who wants to keep information about their pregnancy status private may want to take steps such as utilizing a VPN that masks one's IP address, using internet search providers that promise not to track individuals, and downloading browser extensions that block tracking.³⁴² Other suggestions include checking privacy set-

ucts—can become circumstantial evidence.” (citing Jay Greene, *Tech Giants Have to Hand Over Your Data When Federal Investigators Ask. Here's Why.*, WASH. POST (June 15, 2021), <https://www.washingtonpost.com/technology/2021/06/15/faq-data-subpoena-investigation/> [<https://perma.cc/HMQ7-BFPS>]); Manuela López Restrepo, *Does Your Rewards Card Know If You're Pregnant? Privacy Experts Sound the Alarm*, NPR (Aug. 13, 2022), <https://www.npr.org/2022/08/13/1115414467/consumer-data-abortion-roe-wade-pregnancy-test-rewards-card-target-walgreens> [<https://perma.cc/6285-VH42>].

³³⁸ Vertesi, *supra* note 335 (noting how the author's husband saw a warning that he could be reported to authorities for making “excessive transactions” using gift cards, something they were doing to attempt to hide their pregnancy status from advertisers).

³³⁹ See, e.g., Timothy Summers, *Protect Your Privacy During Turbulent Times: A Hacker's Guide to Being Cyber-Safe*, ASSOCIATED PRESS (Dec. 7, 2016), <https://apnews.com/article/44bda26a654b4957a71e58146c7f14b9> [<https://perma.cc/B4ZP-4WPH>] (noting that it is “less straightforward” to search the internet privately).

³⁴⁰ CAHN & MANIS, *supra* note 26, at 3 (noting that “[i]nternet search engines are a particularly potent tool for tracking pregnant people”).

³⁴¹ Bobby Allyn, *Privacy Advocates Fear Google Will Be Used to Prosecute Abortion Seekers*, NPR (July 11, 2022), <https://www.npr.org/2022/07/11/110391316/google-data-abortion-prosecutions> [<https://perma.cc/2762-7BX5>].

³⁴² For example, as part of executive branch privacy efforts post-*Dobbs*, the HHS Office for Civil Rights issued patient guidance regarding ways to increase privacy on mobile devices. *Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet*, U.S. DEP'T OF HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html> [<https://perma.cc/G3RF-YQU3>] (June 29, 2022); see also Barnett, *supra* note 39; CAHN & MANIS, *supra* note 26, at 13–15 (discussing tips to keep pregnancy information private); Leonard, *supra* note 238. Navigating these options is incredibly complex. See, e.g., Summers, *supra* note 339 (discussing several strategies from an “ethical hacker” to maximizing data privacy). Even when something seems like it will be private and protected, it may not be. See, e.g., JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 170–71 (2014) (noting that internet browser settings, such as “Incognito” or “InPri-

tings across devices, considering a more private email service, and even using a burner phone.³⁴³

All of these steps are complex and may be even less accessible to those with lower income or lower tech literacy.³⁴⁴ Some means to protect privacy cost money, such as using cash for goods, traveling to brick-and-mortar stores, and purchasing privacy-enhancing technology. Not everyone will have the ability to make these financial choices. Additionally, those with lower literacy may have a harder time understanding the complex privacy policies of various apps and organizations, and thus have a harder time determining who they can trust with their data. Given that investigations and prosecutions of pregnancy outcomes disproportionately fall on lower-income women and women of color, it is especially problematic that privacy is disproportionately available to the privileged.³⁴⁵

The problem is that even if a pregnant individual goes through all of these steps, the very fact that she interacts with the medical system could still place her privacy at risk. Bringing a phone to a doctor's office could key in companies and data brokers to the patient's location via GPS, Wi-Fi signals,³⁴⁶ or even internal phone sensors.³⁴⁷ Therefore, a pregnant woman may want to leave her cell phone at home while going to the doctor. Yet, simple interactions with the medical system create privacy risks. Filling out pre-appointment health information without carefully reading privacy notices could open one up to unwanted sharing of health information.³⁴⁸ Even the fact of simply getting a prescription could theoretically be accessed and used by law enforcement³⁴⁹ or

vate Browsing" do little other than prevent those with access to your computer from seeing which websites you visited).

³⁴³ Barnett, *supra* note 39. Keeping a burner phone actually private, however, is much more difficult than one might imagine. *See, e.g.*, ANGWIN, *supra* note 342, at 144–46 (explaining the difficulties that the author had in trying to keep her burner phone delinked from her personal identity).

³⁴⁴ Dellinger & Pell, *supra* note 241.

³⁴⁵ *See, e.g.*, McDonald, *supra* note 334 (“People who are most vulnerable to online privacy encroachment and to the use or abuse of their data have traditionally been those society deems less worthy of protection: people without means, power or social standing.”); *see also supra* Subsection II.B.1.

³⁴⁶ *See, e.g.*, Prince, *supra* note 47, at 51 (explaining that a person's location can be ascertained by using “a phone's available Wi-Fi connections and their associated signal strength”).

³⁴⁷ Susan Landau, *FTC Lawsuit Spotlights a Major Privacy Risk: From Call Records to Sensors, Your Phone Reveals More About You Than You Think*, THE CONVERSATION, <https://theconversation.com/ftc-lawsuit-spotlights-a-major-privacy-risk-from-call-records-to-sensors-your-phone-reveals-more-about-you-than-you-think-189618> [<https://perma.cc/H52Y-W9PB>] (Aug. 29, 2022).

³⁴⁸ Alex R. Rosenblat, Opinion, *I Declined to Share My Medical Data with Advertisers at My Doctor's Office. One Company Claimed Otherwise*, STAT (Apr. 7, 2023), <https://www.statnews.com/2023/04/07/medical-data-privacy-phreesia/> [<https://perma.cc/5CD4-KT7U>].

³⁴⁹ This could come up several ways in the context of reproductive rights. First, if a pregnant woman is prescribed a medication that is tracked through prescription-drug monitoring programs (PDMPs), such as opioids, the prescription could be accessible to law enforcement and used to show potential harm to a fetus. Or, if abortion medication is ever classified as a controlled substance, it

shared with advertisers.³⁵⁰ In our incredibly leaky data environment, making an appointment to see a doctor could share private information with companies.³⁵¹ In one example, the hospital appointment-scheduling website sent Facebook information regarding the doctor's name and specialty as well as the search term used to identify the doctor—in this instance, “pregnancy termination.”³⁵² Thankfully, HHS has recently been limiting this practice.³⁵³

* * * *

could also potentially be accessed by law enforcement via PDMPs. *See generally* Jennifer D. Oliva, *Prescription-Drug Policing: The Right to Health-Information Privacy Pre- and Post-Carpenter*, 69 DUKE L.J. 775 (2020) (discussing law enforcement access to PDMP databases). Moreover, and potentially more concerning, most states have enacted PDMP laws that allow them to track prescription medications that are not controlled substances but nonetheless deemed “drugs of concern.” Jennifer D. Oliva, *Dosing Discrimination: Regulating PDMP Risk Scores*, 110 CALIF. L. REV. 47, 76–77, 77 & n.172 (2022). As such, most states can begin tracking medication abortion by regulatory action (e.g., by amending their list of PDMP-tracked “drugs of concern”). *See id.* Beyond PDMPs, however, prescriptions housed within one's medical records could also potentially be accessed by law enforcement. Boodman et al., *supra* note 244. Even policies that allow for sharing of de-identified prescription data could threaten patient privacy. *See* Christopher R. Smith, *Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information*, 36 VT. L. REV. 931, 933 (2012); Teresa Carr, *Your Prescriptions Are Not a Secret*, CONSUMER REPS. (Mar. 18, 2016), <https://www.consumerreports.org/health-privacy/prescriptions-not-secret-a1139767945/> [<https://perma.cc/QT3-W4SN>]. To the extent that this is occurring, an individual's prescription history can easily give direct evidence of reproductive health status. For example, stopping birth control can indicate that a person is trying to conceive. A prescription for mifepristone shows that a person likely underwent a medication abortion or had an incomplete miscarriage, and thus needed to take medication abortion drugs to expel the fetal tissue. Anyone undergoing IVF treatment will have a record of various prescriptions assisting in this process. It is beyond the scope of this Article to discuss the ways that data from medical records can leak out into the general data ecosystem, although this is also occurring on a regular basis.

³⁵⁰ For example, the FTC has recently filed suit against GoodRX, an online pharmacy, for violations of its privacy policy. Complaint for Permanent Injunction, Civil Penalties, & Other Relief at 1–4, *United States v. GoodRX Holdings, Inc.*, No. 23-cv-460 (N.D. Cal. Feb. 1, 2023) (“GoodRx repeatedly violated [its] promises, however, by sharing sensitive user information with third-party advertising companies”); *see also* Todd Feathers, *The FTC Is Taking on Telehealth's Data Sharing Problem—Starting with GoodRx*, THE MARKUP (Feb. 1, 2023), <https://themarkup.org/pixel-hunt/2023/02/01/the-ftc-is-taking-on-telehealths-data-sharing-problem-starting-with-goodrx> [<https://perma.cc/6NMG-L3U2>].

³⁵¹ Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> [<https://perma.cc/2BPX-RCG4>] (finding Facebook trackers on thirty-three hospital scheduling pages and noting that this could very well be a violation of HIPAA). A class-action lawsuit has been filed related to this practice. Susan Morse, *Meta Platforms Sued for Alleged Unlawful Collection of Patient Data*, HEALTHCARE FIN. (June 27, 2022), <https://www.healthcarefinancenews.com/news/meta-platforms-sued-alleged-unlawful-collection-patient-data> [<https://perma.cc/9CQX-4B7F>].

³⁵² Feathers et al., *supra* note 351.

³⁵³ *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> [<https://perma.cc/NS47-KC6P>] (Dec. 1, 2022).

As one commentator aptly wrote, “if people really wanted to keep all their information concealed, they would have to live in a shack in the woods.”³⁵⁴ Privacy self-management is not a perfect solution to maintain reproductive health privacy. And although complete privacy self-management is impossible, it is not fruitless for individuals to take steps to clean up their data privacy hygiene.³⁵⁵ Making information about reproductive health more difficult to access and infer could make it harder for companies to target individuals with unwanted ads, less likely that employers can access information, and more difficult for law enforcement to investigate pregnancy outcomes. These individual efforts, however, should not be the only line of defense for reproductive health privacy.

B. Company Privacy Management

The second line of defense in the reproductive health privacy realm is company practice and good will. The EFF, a nonprofit digital rights group, recommends that companies follow a series of steps to shore up the privacy of their applications and services, related to both data practices and law enforcement access.³⁵⁶ In terms of data practices, the EFF has several key recommendations, such as allowing pseudonymous access, stopping behavioral tracking, deleting data regularly, encrypting data, limiting sharing, and minimizing the collection of location data.³⁵⁷ As it notes, “if you build it, they will come—so don’t build it, don’t keep it, dismantle what you can, and keep it secure.”³⁵⁸ EFF also recommends that companies push back against law enforcement by challenging improper warrants or subpoenas.³⁵⁹

Post-*Dobbs*, several companies have publicly explained how they are going to change data collection and handling practices to improve privacy for users. These steps came after much public debate regarding the privacy implications of

³⁵⁴ Solove, *supra* note 102, at 30.

³⁵⁵ Nor should policies that give individuals more control and choice about how their data is collected and used be stopped. Solove, *supra* note 69, at 1899–900 (arguing that privacy self-management, despite all its flaws, should not be abandoned).

³⁵⁶ Corynne McSherry & Katharine Trendacosta, *What Companies Can Do Now to Protect Digital Rights in a Post-Roe World*, ELEC. FRONTIER FOUND. (May 10, 2022), <https://www.eff.org/deeplinks/2022/05/what-companies-can-do-now-protect-digital-rights-post-roe-world> [<https://perma.cc/9R2Y-Y36V>].

³⁵⁷ *Id.*

³⁵⁸ *Id.* (capitalization omitted).

³⁵⁹ *Id.*

technologies like Google and Femtech.³⁶⁰ Other companies had designed their products with privacy in mind long before the *Dobbs* decision broke.³⁶¹

Just one week after the *Dobbs* decision came down, Google announced that if one of its users visited an abortion clinic, it would delete this information from their location history.³⁶² Notably, this new data practice included not only abortion clinics, but other sensitive reproductive health-related locations, such as fertility clinics.³⁶³ It is important to note, however, that this approach can carry risks as well—a gap in location history may allow the inference that one has visited a sensitive location.

Following the receipt of congressional letters expressing concern about location information related to reproductive care,³⁶⁴ two data brokers agreed to cease selling the location data of those who visit abortion clinics.³⁶⁵ In addition, Apple users were already more insulated from geofence warrants because the company does not store location data in a format that allows them to respond to law enforcement requests.³⁶⁶

In the Femtech space, Flo, the same company that recently settled with the FTC over privacy violations,³⁶⁷ announced that it would create an “Anonymous Mode” where users could utilize services without inputting their name or email address.³⁶⁸ This could prevent Flo from being able to comply with

³⁶⁰ See, e.g., Gebhart & Barnett, *supra* note 250; *supra* Subsection III.A.1.

³⁶¹ See generally Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1411 (2011) (discussing the concept of “privacy by design,” where companies “promote consumer privacy throughout their organizations and at every stage of the development of their products and services”).

³⁶² Nico Grant, *Google Says It Will Delete Location Data When Users Visit Abortion Clinics*, N.Y. TIMES (July 1, 2022), <https://www.nytimes.com/2022/07/01/technology/google-abortion-location-data.html> [<https://perma.cc/7GM3-985H>].

³⁶³ *Id.* Google also included “other sensitive locations” that were unrelated to reproductive health, such as “domestic violence shelters, [and] addiction treatment facilities.” *Id.*

³⁶⁴ See generally Letter from Elizabeth Warren et al., U.S. Sens., to Auren Hoffman, Chief Exec. Officer, SafeGraph, Inc. (May 17, 2022) (on file with author); Letter from Elizabeth Warren et al., U.S. Sens., to Noam Ben-Zvi, Chief Exec. Officer, Placer.ai (May 17, 2022) (on file with author).

³⁶⁵ Press Release, Elizabeth Warren, U.S. Sen., Warren Announces Two Key Data Brokers’ Commitment to Permanently Stop Selling Location Data of People Seeking Abortion Services (July 7, 2022), <https://www.warren.senate.gov/newsroom/press-releases/warren-announces-two-key-data-brokers-commitment-to-permanently-stop-selling-location-data-of-people-seeking-abortion-services> [<https://perma.cc/DV5Y-54HM>].

³⁶⁶ Ng, *supra* note 237. These users could presumably still be at risk, however, if they allow another third party to access location data, such as by using a navigation app that has less strict privacy protections to get directions to an abortion clinic.

³⁶⁷ See *supra* Section I.C.

³⁶⁸ Flo App (@flotracker), TWITTER (June 24, 2022, 2:39 PM), <https://twitter.com/flotracker/status/1540404337842995200> [<https://perma.cc/G7AL-6LAY>].

requests to identify a user by name or email.³⁶⁹ Changes to privacy policies within the Femtech space are not isolated. “The picture . . . is one of companies scrambling to transform—building out legal teams, racing to design new privacy-protecting products, and aiming to communicate more clearly about how they handle data and provide care in the face of swirling distrust of digital health tools.”³⁷⁰ Other less-well-known Femtech apps are designed to align with privacy and security best practices from their genesis.³⁷¹

Organizations more directly linked with the provision of reproductive healthcare services have also been forced to think more carefully about their data practices. For example, following reports that website tracking tools sent Facebook information about scheduled health appointments, including abortions and pregnancy check-ups, several hospitals deleted the tracking tool from their websites.³⁷² Similarly, Planned Parenthood also announced that it would remove marketing trackers from abortion-related search pages after reports emerged that IP addresses could be shared with third-party tracking companies.³⁷³

Even company efforts such as these, however, are not a panacea.³⁷⁴ The strengthening of privacy policies of organizations and tech companies is an unalloyed good. Yet, much like individual privacy self-management, it is not a comprehensive solution to protecting reproductive health privacy for several reasons.

First, there is the real risk that publicized company efforts immediately following the *Dobbs* decision amount to privacy washing—where companies take an action to look like they are meeting a social standard, but fail to address the true underlying problems.³⁷⁵ For example, company choices may limit the ability of law enforcement or advertisers to use geofence techniques surrounding abortion clinics or may limit some aspects of widespread data shar-

³⁶⁹ Amina Kilpatrick, *Period Tracker App Flo Developing ‘Anonymous Mode’ to Quell Post-Roe Privacy Concerns*, NPR (June 30, 2022), <https://www.npr.org/2022/06/30/1108814577/period-tracker-app-flo-privacy-roe-v-wade> [https://perma.cc/VVR3-KSDA].

³⁷⁰ Palmer & Ross, *supra* note 221.

³⁷¹ Catherine Roberts, *These Period Tracker Apps Say They Put Privacy First. Here’s What We Found.*, CONSUMER REPS., <https://www.consumerreports.org/health-privacy/period-tracker-apps-privacy-a2278134145/> [https://perma.cc/Y52N-NS9J] (Aug. 30, 2022).

³⁷² Feathers et al., *supra* note 351.

³⁷³ Tatum Hunter, *Planned Parenthood Suspends Marketing Trackers on Abortion Search Pages*, WASH. POST (June 30, 2022), <https://www.washingtonpost.com/technology/2022/06/30/planned-parenthood-privacy-data/> [https://perma.cc/U44L-M2XJ].

³⁷⁴ Ng, *supra* note 237 (explaining that privacy experts note that there could be covert abortion locations not deleted from Google’s databank because they are not known to Google, but that could be known to police). It is one of the reasons why some are asking Google to simply stop collecting and retaining all location data rather than attempting a piecemeal approach.

³⁷⁵ Margot E. Kaminski, *The Case for Data Privacy Rights (Or, Please, a Little Optimism)*, 97 NOTRE DAME L. REV. REFLECTION 385, 388–89 (2022), available at <https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=2550&context=faculty-articles> [https://perma.cc/NVG5-66DU].

ing. But this just focuses on one aspect of the reproductive health data ecosystem. “While many of the country’s largest tech companies have been quick to voice support for pregnant employees, few have addressed how their own data is going to be used against abortion seekers.”³⁷⁶ More holistic company changes to data practices are needed.

Second, changes to company policies or clarifications of data practices ultimately still require individuals to learn about these practices and self-manage privacy through their choices of which products to use.³⁷⁷ As discussed above, however, this is no easy task—especially when companies are advertising seemingly attractive privacy practices to lure customers despite still having gaps in their policies. For example, one Femtech company, Stardust, entered the market following the *Dobbs* decision and specifically promoted their data practices by announcing that they will never sell user data.³⁷⁸ Yet, at least one version of their privacy policy also indicated that they would provide user data to law enforcement “whether or not legally required.”³⁷⁹

The recommendations suggested by the EFF to protect user privacy, such as refraining from sharing data with third parties and tracking behavior, flies in the face of the business models of many companies that rely on targeted advertising for marketing, or sale of data for profit.³⁸⁰ Thus, although some companies may strengthen privacy practices or even see it as a marketing device to advertise

³⁷⁶ CAHN & MANIS, *supra* note 26, at 10–13 (discussing the myriad ways that data housed by Google, Meta, Apple, Amazon, Femtech companies, and retailers is still accessible for investigation by law enforcement).

³⁷⁷ See generally Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017) (discussing how privacy principles that give users more control over their data are necessary, but not sufficient, for true privacy protection).

³⁷⁸ Poli, *supra* note 331.

³⁷⁹ *Popular Stardust Period Tracker Will Hand Over Users Data Without a Warrant*, IT WORLD CAN. (June 28, 2022), <https://www.itworldcanada.com/post/popular-stardust-period-tracker-will-hand-over-users-data-without-a-warrant> [<https://perma.cc/MQJ4-BPL6>]. Stardust’s privacy policy appears to have been reworded since. The policy, effective since October 19, 2022, now states that “[w]hile the Company may be legally required to produce information in response to . . . [information requests from law enforcement] or legal process, any Health Data that the Company is required to share will remain anonymous such that it cannot be linked back to you.” *We Do Not and Will Not Sell Your Data. Period.*, STARDUST, <https://stardust.app/privacy-policy.html> [<https://perma.cc/9TZ2-VT8G>]. The company also was criticized for its description of its encryption practices. Leigh Mc Gowran, *Period Tracker Stardust Rolls Back Encryption Claims Amid Scrutiny*, SILICON REPUBLIC (June 28, 2022), <https://www.siliconrepublic.com/enterprise/stardust-period-app-encryption> [<https://perma.cc/RE7L-3EFY>].

³⁸⁰ See, e.g., Alfred Ng, *Data Brokers Resist Pressure to Stop Collecting Info on Pregnant People*, POLITICO (Aug. 1, 2022), <https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988> [<https://perma.cc/FNL4-A6DZ>] (noting that, following *Dobbs*, data brokers have continued to amass data identifying pregnant individuals, despite pressure from lawmakers to end these practices).

strong data protection, company-driven action will never be a comprehensive solution unless the underlying business models are drastically overhauled.³⁸¹

C. Regulating and Enforcing Privacy

Self-management and new company practices can limit the amount of reproductive health data that flows into the data ecosystem. Importantly, however, more is needed to solve the problem. Reproductive health surveillance will continue unless there is wholesale, radical change of our underlying data ecosystem. This, of course, is a difficult ask—there have been some key legislative efforts, but wholesale privacy regulation faces pushback and challenges.³⁸²

This Article highlights the need for four key aspects of reproductive health privacy regulation: (1) regulation of data brokers and the data ecosystem fueled by monetization; (2) regulation of both sensitive information and information that can be used to infer sensitive information; (3) regulation of data collection itself; and (4) regulation across the states.³⁸³ Proposed bills in Congress meet some of these needs, but not all.³⁸⁴ Despite these gaps, there is merit in continuing the push for legislative change. Any increase in privacy protection is better than nothing at all. Nevertheless, we also need an honest conversation about the remaining gaps in the system and what needs to be done to truly protect reproductive health privacy.

1. Minimizing Reproductive Health Surveillance

Reproductive health surveillance is omnipresent, expansive, and extremely problematic. The *Dobbs* decision has shed light on the risks of widespread collection of data and has created grave threats of criminalization for those seeking abortions and those who assist them. Additionally, the reproductive

³⁸¹ See generally Gilman, *supra* note 58.

³⁸² In addition to proposed legislation, the executive branch has also taken several steps to clarify existing privacy rights, including an Executive Order by President Biden titled “Protecting Access to Reproductive Healthcare Services.” Exec. Order No. 14,076, 87 Fed. Reg. 42053 (July 8, 2022). Members of Congress have also encouraged further executive branch action and called on companies to improve their data practices; for example, the same day that the Supreme Court released the *Dobbs* decision, several members of Congress wrote a letter to the Chair of the FTC, Lina Khan, encouraging her to investigate both Apple and Google regarding certain data collection practices. Brian Fung, *Apple and Google Should Face FTC Probe Over Ad Practices That Could End Up Harming Abortion-Seekers, US Lawmakers Say*, CNN (June 24, 2022), <https://www.cnn.com/2022/06/24/tech/apple-google-ftc-probe-abortion-ads/index.html> [<https://perma.cc/LE7K-XRF6>]. The letter details how the tracking techniques of the large tech companies are especially problematic post-*Dobbs*. *Id.* Other congressional efforts have been discussed throughout this Article. See, e.g., Letter from Wyden et al. to Pichai, *supra* note 235, at 1–2; Letter from Warren & Markey to Bason, *supra* note 322, at 1–2.

³⁸³ See *infra* Subsection IV.C.1.

³⁸⁴ See *infra* Subsection IV.C.2.

health data ecosystem generates risks of data access by employers, insurers, and everyday citizens, and creates implications for all reproductive health outcomes.

Privacy protections are complex and require many nuanced elements to be meaningful.³⁸⁵ This Article focuses in on four key elements: regulation of data brokers,³⁸⁶ regulation of inferred information,³⁸⁷ regulation of data collection,³⁸⁸ and regulation across the states.³⁸⁹

a. Regulation of Data Brokers

Much of the current debate post-*Dobbs* has focused on concerns about how law enforcement may gain access to reproductive health data.³⁹⁰ As this Article shows, however, there are also great harms related to private company collection of data. These two—private and law enforcement data collection—are inextricably linked. “Information bought and sold by the largely unregulated data-broker industry is increasingly not only targeting pregnant people with ads, but a tool for targeting them for arrest.”³⁹¹ Law enforcement has been known to purchase data as part of their investigations. Additionally, if the data is available and there is probable cause, law enforcement could potentially gain lawful access to existing data through warrants.³⁹² Although there may

³⁸⁵ For example, regulation related to other issues, such as re-identification, preemption, or non-discrimination, may also be essential to bolstering protections. Gennie Gebhart, *EFF's Recommendations for Consumer Data Privacy Laws*, ELEC. FRONTIER FOUND. (June 17, 2019), <https://www.eff.org/deeplinks/2019/06/effs-recommendations-consumer-data-privacy-laws> [<https://perma.cc/P53M-7GD6>]. Additionally, many proposed privacy laws strengthen individual rights, such as the right to correct or delete information. *See, e.g.*, CATHY COSGROVE & KAVYA NAGUMOTU, INT’L ASS’N OF PRIV. PROS., 2021 PROPOSED COMPREHENSIVE US PRIVACY LEGISLATION 1 (2021), https://iapp.org/media/pdf/resource_center/2021_proposed_comprehensive_us_privacy_legislation_chart.pdf [<https://perma.cc/R29Y-R67N>] (comparing proposals for federal privacy laws). These individual rights can be meaningful and important, even if they follow the model of privacy self-management. This is not to say that these important rights to privacy self-management should be excluded from privacy protections. Solove, *supra* note 69, at 1899–900 (arguing that, despite its flaws, privacy self-management should not be completely abandoned); *see also* Kaminski, *supra* note 375, at 389–90 (arguing that, although other data protections are also needed, individual privacy tools remain important). Still, this Article focuses on other protections, particularly on the duties of data holders, given the need to move beyond privacy self-management to truly protect reproductive health data.

³⁸⁶ *See infra* Subsection IV.C.1.a.

³⁸⁷ *See infra* Subsection IV.C.1.b.

³⁸⁸ *See infra* Subsection IV.C.1.c.

³⁸⁹ *See infra* Subsection IV.C.1.d.

³⁹⁰ *See supra* Section III.A.

³⁹¹ CAHN & MANIS, *supra* note 26, at 4.

³⁹² *See* Dellinger & Pell, *supra* note 241 (discussing the “[l]imited [e]fficacy” of the Fourth Amendment and warrant requirements post-*Dobbs*). Additionally, some data may be directly accessible to law enforcement under the “[t]hird-[p]arty [d]octrine,” whereby individuals lose their expectation of privacy if information is shared with a third party. John Villasenor, *What You Need to Know*

still be Fourth Amendment limitations to accessing the data, such as arguments about the unconstitutionality of geofence warrants,³⁹³ the more data that exists the more that may be accessible to law enforcement.

Similarly, a law that targets companies that collect private data, without addressing data brokers and the role they play in aggregating and further disseminating information, will not completely fill the gaps. Therefore, at a minimum, privacy laws must address the companies collecting data, the data brokers, and law enforcement access of data beyond warrants, such as informal requests or purchases.

For example, one bill introduced in Congress prior to *Dobbs* is now even more crucial. Titled the Fourth Amendment Is Not for Sale Act, the bill would limit law enforcement's ability to purchase private data from data brokers as a way around warrant requirements.³⁹⁴ There are already rules for how law enforcement interacts with phone and social media companies, so this bill would fill in the gap with respect to data brokers.³⁹⁵ Although the bill makes it more difficult for law enforcement to access reproductive health data *without* a warrant, it does nothing to limit the amount of data available with a warrant—data that is also available to advertisers and anti-abortion activists. Other legislation would still be needed to fill this gap. Thus, although there are merits to bills like this, broader solutions are needed.

b. Regulation of Inferred Information

Given the ability of companies to infer reproductive health information from innocuous data points, any regulation must address both the sensitive data and the sensitive inferences made using non-sensitive data. For example, a law that is narrowly tailored to only protect information related to abortion may still leave individuals who experience miscarriage open to threats.³⁹⁶ Sim-

About the Third-Party Doctrine, THE ATLANTIC (Dec. 30, 2013), <https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/> [<https://perma.cc/9KDM-6574>]. Following the Supreme Court's 2018 decision in *Carpenter v. United States*—which held that there is a reasonable expectation of privacy in cellphone location data, given the sensitive information it could uncover—there are questions remaining as to how the third-party doctrine will play out in other contexts. 138 S. Ct. 2206, 2217 (2018); Conti-Cook, *supra* note 203, at 40–45; Fowler & Ulrich, *supra* note 26 (manuscript at 53–54) (discussing how the *Carpenter* ruling may not address instances where information is voluntarily provided to a third party, such as a Femtech app).

³⁹³ Lavoie, *supra* note 237.

³⁹⁴ Fourth Amendment Is Not for Sale Act, S. 1265, 117th Cong. § 1 (2021).

³⁹⁵ Press Release, Zoe Lofgren, U.S. Rep., Nadler, Lofgren Introduce Bicameral Fourth Amendment Is Not for Sale Act (Apr. 21, 2021), <https://lofgren.house.gov/media/press-releases/nadler-lofgren-intro-bicameral-fourth-amendment-not-sale-act> [<https://perma.cc/8SU2-VPL3>].

³⁹⁶ See *supra* Subsection III.A.2.

ilarly, legislation that protects existing health data may not fully protect individuals in situations where their data is used to infer health status.³⁹⁷

Two congressional bills introduced in June 2022 following the *Dobbs* decision highlight efforts to address these concerns. The Health and Location Data Protection Act would prevent data brokers from selling both location and health data.³⁹⁸ It has several strengths, including, notably, prohibiting the sale of location and health information, even when inferred.³⁹⁹ Thus, it would protect reproductive health information directly shared with companies. But it would also protect against data brokers selling information related to reproductive health that was indirectly inferred, using algorithms or other techniques.⁴⁰⁰

The other law proposed in June of 2022, the My Body, My Data Act, would protect a wide range of reproductive and sexual health data.⁴⁰¹ It covers everything from information about medications—including contraceptives, abortifacients, and others “related to reproductive health”—to information about use of reproductive health services, to data that is “derived or extrapolated from non-health information (such as proxy, derivative, inferred, emergent, or algorithmic data).”⁴⁰²

c. Regulation of Data Collection

Privacy laws can be designed to maximize either upstream or downstream protections.⁴⁰³ Upstream regulation seeks to limit the possible threat from data,

³⁹⁷ Prince, *supra* note 47, at 79.

³⁹⁸ Health and Location Data Protection Act of 2022, S. 4408, 117th Cong. (2022). The bill also bolsters FTC enforcement of data practices, including through increased funding. Press Release, Elizabeth Warren, U.S. Sen., Warren, Wyden, Murray, Whitehouse, Sanders Introduce Legislation to Ban Data Brokers from Selling Americans’ Location and Health Data (June 15, 2022), <https://www.warren.senate.gov/newsroom/press-releases/warren-wyden-murray-whitehouse-sanders-introduce-legislation-to-ban-data-brokers-from-selling-americans-location-and-health-data> [<https://perma.cc/5FPH-BEPN>].

³⁹⁹ S. 4408 § 2(a). The bill, in relevant part, reads:

It shall be unlawful for a data broker to sell, resell, license, trade, transfer, share, or otherwise provide or make available any of the following forms of data, whether declared or inferred, of an individual: (1) Location data. (2) Health data. (3) Other categories of data identified by the Commission that address or reveal a category of data described in paragraphs (1) and (2).

Id. § 2(a)(1)–(3). There are several exceptions for data that is HIPAA compliant, newsworthy and of public concern, or disclosed following valid authorization. *Id.* § 2(b)(1)–(3).

⁴⁰⁰ *See id.* § 2(a).

⁴⁰¹ My Body, My Data Act of 2022, H.R. 8111, 117th Cong. (2022).

⁴⁰² *Id.* § 6(6)(D), (G).

⁴⁰³ Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 103 (2014).

such as by limiting the collection of the data in the first instance.⁴⁰⁴ For example, some privacy regimes, such as the European Union's General Data Protection Regulation (GDPR), require that data only be collected for legitimate purposes and that the data collected be narrowly tailored to those purposes.⁴⁰⁵ Downstream regulations, on the other hand, focus on the use of data once it is collected, such as by imposing security requirements, or limiting the disclosure or dissemination of data.⁴⁰⁶

In the context of reproductive health privacy, upstream regulation that limits the collection of information is the most protective, especially given the post-*Dobbs* threat of warrants or subpoenas that could compel disclosure of information otherwise protected by privacy laws.⁴⁰⁷ As in the case of privacy self-management, even if harms from disclosure cannot be completely prevented, minimizing the collection of data can lessen the potential harms.

Nevertheless, given that reproductive health information can be inferred from many different innocuous data points,⁴⁰⁸ limiting collection of reproductive health information will only protect against direct sharing—it would not necessarily prevent a data broker or other entity from aggregating information to infer reproductive health status. One way to limit aggregation is to prohibit entities from profiling an individual's health.⁴⁰⁹ This type of law could potentially stop data brokers from creating marketing categories, such as “pregnant” or “abortion-minded”—labels that could be of interest to advertisers, anti-abortion activists, and law enforcement alike.

One of the proposed bills, in particular, seeks to address wide-scale collection of reproductive data. The My Body, My Data Act, discussed above, aims to create a federal standard for protecting reproductive health data.⁴¹⁰ The proposed legislation provides many rights for privacy self-management, such as the rights of access and deletion,⁴¹¹ as well as enhanced privacy notices.⁴¹²

⁴⁰⁴ *Id.*

⁴⁰⁵ Council Regulation 2016/679, 2016 O.J. (L 119) 1, 35–36.

⁴⁰⁶ Terry, *supra* note 403, at 103.

⁴⁰⁷ For example, both the Health and Location Data Protection Act and the My Body, My Data Act, discussed above, allow for law enforcement collection of reproductive health data through warrants or subpoenas. Health and Location Data Protection Act of 2022, S. 4408, 117th Cong. § 2(b) (2022); H.R. 8111 § 9.

⁴⁰⁸ See, e.g., Prince, *supra* note 47, at 47; Terry, *supra* note 403, at 79–80; Marks, *supra* note 47, at 997.

⁴⁰⁹ Bari & O'Neill, *supra* note 127 (arguing that health privacy laws should prevent data from being utilized to “create or commercialize health profiles of the individual”); Prince, *supra* note 47, at 66–69.

⁴¹⁰ See generally H.R. 8111 (stating that its purpose is to “protect the privacy of personal reproductive or sexual health information”).

⁴¹¹ *Id.* § 3(a)–(b).

⁴¹² *Id.* § 4(c) (mandating a comprehensive “clear and conspicuous” privacy policy from regulated parties).

The main power of the bill, however, is that it flips the default position that has become so entrenched in the United States.⁴¹³ Rather than allow collection and use of personal data unless specifically prohibited—as is the current default—the My Body, My Data Act begins by prohibiting a covered entity from collecting, retaining, using, or disclosing reproductive or sexual health information.⁴¹⁴ The only exceptions to this broad bar are if the company receives the express consent of the individual or if the information is necessary to provide a product or service.⁴¹⁵ This bill therefore employs both an upstream strategy (as it relates to limiting collection) and a downstream strategy (as it relates to limiting usage and disclosure).

Of course, not all collections and usages of reproductive health data are negative. For example, access to reproductive health data allows researchers to conduct important studies that can improve health. Data tracking also allows researchers to better understand the impact of law and policy on health.⁴¹⁶ Legislation drafters, therefore, may want to be wary of unintentionally preventing beneficial uses of reproductive health data by creating broad prohibitions on the use or disclosure of data.

d. Regulation Across States

Many states where abortion remains legal are also thinking about increasing privacy protections within their jurisdictions.⁴¹⁷ Nevertheless, a federal

⁴¹³ *Id.* § 2(a). HIPAA begins with the standard that health information should not be shared without specific patient authorization, absent a handful of exceptions. 45 C.F.R. § 164.502(a) (2021). One of the central exceptions is that patient information can be shared “[f]or treatment, payment, or health care operations.” *Id.* § 164.502(a)(1)(ii); see Prince, *supra* note 47, at 77 (“Effectively, this [standard] means that individually identifiable patient information is shared relatively freely within the healthcare entity and business associates themselves, [but that] disclosure to noncovered entities is more circumscribed.”). Outside of HIPAA, the baseline is often that data can generally be collected and shared unless explicitly prohibited—often with few prohibitions. Prince, *supra* note 47, at 48.

⁴¹⁴ H.R. 8111 § 2(a).

⁴¹⁵ *Id.* § 2(a)(1)–(2). Additionally, “express consent” is defined strictly. *Id.* § 6(4) (defining “express consent” as obtaining “informed, opt-in, voluntary, specific, and unambiguous written consent”). For example, it does not include “[h]overing over, muting, pausing, or closing a given piece of content.” *Id.* § 6(4)(B)(ii).

⁴¹⁶ See, e.g., Conti-Cook, *supra* note 203, at 26–28 (using Google Trends to compare the frequency of searches for “abortion pills” in states generally, and in states with the most abortion restrictions more specifically); Poliak et al., *supra* note 175, at 1003 (exploring trends in internet searches for abortion medications after the leaked *Dobbs* draft decision).

⁴¹⁷ CAHN & MANIS, *supra* note 26, at 7–9; Nik Popli & Vera Bergengruen, *Lawmakers Scramble to Reform Digital Privacy After Roe Reversal*, TIME (July 1, 2022), <https://time.com/6193224/abortion-privacy-data-reform/> [<https://perma.cc/3X3T-C55L>]; Adam Schwartz, *EFF to California Governor: Protect Abortion Data Privacy*, ELEC. FRONTIER FOUND. (Sept. 8, 2022), <https://www.eff.org/deeplinks/2022/09/eff-california-governor-protect-abortion-data-privacy> [<https://perma.cc/8KGX-NQPG>].

solution is needed to ensure that individuals have reproductive health privacy across all states, and perhaps most importantly, in those most likely to criminalize pregnancy outcomes and reproductive health choices. These are likely not the states that will bolster reproductive health privacy, leaving many individuals across the nation at risk. Additionally, there are many expected battles regarding cross-border abortions, where individuals from a restrictive state travel to a state where abortion is legal.⁴¹⁸ Stronger privacy protections in the states providing care cannot necessarily prevent data collection in the individual's home state, although there are state-level efforts to limit data transfer from a protective state to a restrictive state.⁴¹⁹

2. The American Data Privacy and Protection Act (ADPPA)

The bills described above are relatively targeted toward a specific privacy concern, be it law enforcement purchasing private data from brokers or the need to protect reproductive health and location information. A comprehensive privacy bill could also effectively protect reproductive health privacy and address other data that is worthy of protection, such as mental health status, sexual preference, or history of domestic abuse. In the 117th Congress alone, members of Congress introduced sixty-two privacy-related bills, including thirteen focused on health privacy.⁴²⁰ One bill in particular, the American Data Privacy and Protection Act (ADPPA), was introduced after months of bipartisan negotiations.⁴²¹ It would have established a comprehensive data privacy regime at the federal level for the first time.

The ADPPA was introduced in the House in June 2022 with bipartisan support.⁴²² Although neither chamber voted on the bill, it made its way out of committee, which is the farthest that any comprehensive privacy bill has ever

⁴¹⁸ See generally Cohen et al., *supra* note 130 (exploring the future cross-border battles regarding abortion post-*Dobbs*).

⁴¹⁹ See, e.g., Hayley Tsukayama, *Reproductive Privacy Requires Data Privacy*, ELEC. FRONTIER FOUND. (May 10, 2022), <https://www.eff.org/deeplinks/2022/05/reproductive-privacy-requires-data-privacy> [<https://perma.cc/VT4Z-VMD5>].

⁴²⁰ MÜGE FAZLIOGLU, INT'L ASS'N PRIV. PROS., US FEDERAL PRIVACY LEGISLATION TRACKER: INTRODUCED IN THE 117TH CONGRESS (2021–2022), at 9–11 (2022), https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf [<https://perma.cc/38UF-NCX8>].

⁴²¹ American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); Joseph Duball, *American Data Privacy and Protection Act Heads for US House Floor*, INT'L ASS'N OF PRIV. PROS. (July 21, 2022), <https://iapp.org/news/a/american-data-privacy-and-protection-act-heads-for-us-house-floor/> [<https://perma.cc/W8RT-U3UD>].

⁴²² H.R. 8152; Duball, *supra* note 421; Press Release, U.S. Senate Comm. on Com., Sci. & Transp., What They Are Saying | American Data Privacy and Protection Act (June 15, 2022), <https://www.commerce.senate.gov/2022/6/what-they-are-saying-american-data-privacy-and-protection-act> [<https://perma.cc/744X-UZFP>] (noting the bipartisan support with which the bill was introduced).

advanced in Congress.⁴²³ Importantly, it would make great strides toward each of the four key protections identified in this Article—although a cause of friction with this bill is its efforts to establish a national standard for privacy.⁴²⁴ This Subsection discusses how well the ADPPA addresses each of this Article’s proposed key elements of privacy protection: regulation of data brokers,⁴²⁵ regulation of inferred data,⁴²⁶ regulation of data collection,⁴²⁷ and regulation across states.⁴²⁸

a. ADPPA: Regulation of Data Brokers

The ADPPA applies to most organizations that collect, process, or transfer protected data, and includes both small and large businesses, as well as for- and not-for-profit companies.⁴²⁹ It does not, however, apply to government entities,⁴³⁰ so this law predominately would address the private company side of the reproductive health data ecosystem, as opposed to law enforcement or state collection of information.

b. ADPPA: Regulation of Inferred Data

Because this is a comprehensive privacy bill, the definition of included data is very broad and covers “information that identifies or is linked or reasonably linkable” to a person.⁴³¹ Importantly, this includes derived data, which is defined as “covered data that is created by the derivation of information, data, assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or another source of information or data about an individual or an individual’s device.”⁴³² Additionally, the proposed legislation creates heightened duties related to sensitive data that includes both health and loca-

⁴²³ Duball, *supra* note 421 (describing the ADPPA’s progress out of committee, even after receiving pushback from some legislators).

⁴²⁴ *Id.* (noting that the California congressional delegation worried that a national privacy standard could interfere with their own state privacy laws).

⁴²⁵ See *infra* Subsection IV.C.2.a.

⁴²⁶ See *infra* Subsection IV.C.2.b.

⁴²⁷ See *infra* Subsection IV.C.2.c.

⁴²⁸ See *infra* Subsection IV.C.2.d.

⁴²⁹ American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 2(9)(A) (2022); JONATHAN M. GAFFNEY, CHRIS D. LINEBAUGH & ERIC N. HOLMES, CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152, at 1 (2022). As is common in data privacy laws, the bill exempts companies that are covered entities under HIPAA. H.R. 8152 § 404(a)(3).

⁴³⁰ H.R. 8152 § 2(9)(B)(i)–(iii).

⁴³¹ *Id.* § 2(8)(A); GAFFNEY ET AL., *supra* note 429, at 1.

⁴³² H.R. 8152 § 2(13).

tion information as well as private communications, such as texts, emails, and voice communications.⁴³³

c. ADPPA: Regulation of Data Collection

The bill has several large categories of regulation, including duties of loyalty, transparency requirements, consumer rights, specific protections for minors, rules for third-party data collectors, and civil rights protections related to algorithms, among others.⁴³⁴ For purposes of reproductive health privacy, however, perhaps one of the most important aspects of the bill is its requirement that companies practice data minimization.⁴³⁵ Data minimization—an upstream data strategy—is the idea that data should only be collected, kept, or shared if it is absolutely necessary.⁴³⁶ Under the ADPPA, companies are prohibited from “collect[ing], processing, or transfer[ring]” personal data unless it is reasonably necessary to provide the specific product, or for one of the enumerated permissible purposes.⁴³⁷ Thus, under the specific product category, Femtech apps could collect reproductive health information as is reasonably necessary to provide the period tracking product. But they would be unable to transfer the data further without meeting a permitted purpose or other exception.

Although one permissible purpose under the ADPPA is targeted marketing,⁴³⁸ this does not apply to sensitive data.⁴³⁹ Therefore, sensitive data, including location and reproductive health information, could not be collected or processed for purposes of creating targeted marketing. Furthermore, all individuals must be provided with an opportunity to opt out of targeted marketing.⁴⁴⁰ Additionally, under the bill, one’s sensitive data can only be transferred to a third party under limited circumstances, such as with express consent.⁴⁴¹ A permissible purpose under the proposed law is research that is in the public in-

⁴³³ *Id.* § 2(28)(A)(i)–(xvi). Specifically, “sensitive covered data” is defined to include “[a]ny information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual.” *Id.* § 2(28)(A)(ii).

⁴³⁴ GAFFNEY ET AL., *supra* note 429, at 2–3.

⁴³⁵ H.R. 8152 § 101.

⁴³⁶ *Data Minimization Principle*, INT’L ASS’N OF PRIV. PROS., <https://iapp.org/resources/article/data-minimization-principle/> [<https://perma.cc/B84Y-YU96>].

⁴³⁷ H.R. 8152 § 101(a)(1)–(2). Another category of allowable data collection and use is “[t]o deliver a communication . . . if that communication is reasonably anticipated by the individual within the context of the individual’s interactions with the covered entity.” *Id.* § 101(a)(2), (b)(11).

⁴³⁸ *Id.* § 101(b)(11). This has been critiqued because targeted marketing is “the economic driver of most commercial surveillance in the first place.” Gilad Edelman, *Don’t Look Now, but Congress Might Pass an Actually Good Privacy Bill*, WIRED (July 21, 2022), <https://www.wired.com/story/american-data-privacy-protection-act-adppa/> [<https://perma.cc/D7SU-K6PB>].

⁴³⁹ H.R. 8152 § 102(2).

⁴⁴⁰ *Id.* § 204(c).

⁴⁴¹ *Id.* § 102(3)(A).

terest, thereby adding allowances for beneficial uses of reproductive health data.⁴⁴² Another permissible purpose is to “prevent, detect, protect against, or respond to fraud, harassment, or illegal activity.”⁴⁴³ It is unclear, however, how this provision would be interpreted in the context of a post-*Dobbs* legal landscape.

d. ADPPA: Regulation Across States

In the 117th Congress, the ADPPA had bicameral and bipartisan support, and therefore showed greater promise than many of the proposed privacy laws that have come before it.⁴⁴⁴ Thus, the bill presented an important opportunity to comprehensively regulate information, including reproductive health information, across states. It was also the national nature of this bill, however, that ultimately stymied its passage in Congress.⁴⁴⁵ One of the major sticking points for passage was whether or not the bill should preempt state law, or whether the legislation should provide a floor and allow for stronger state privacy protections.⁴⁴⁶ As drafted, the bill preempted state privacy laws with few exceptions.⁴⁴⁷ This angered representatives from states with their own comprehensive privacy legislation, especially California’s representatives, and caused the bill’s ultimate demise in the last congressional session.⁴⁴⁸

States like California should be able to legislate greater protections for their constituents, but when this is the sticking point, the end result is that millions of individuals are left with little privacy recourse. Despite these challenges, it is crucial that Congress pass a comprehensive privacy bill, such as the ADPPA, to protect reproductive health across the country.

CONCLUSION

Meaningful progress on comprehensive privacy protections at the federal level is sorely needed. There is a vast reproductive health data ecosystem driven by profit motives—monetizing women’s reproductive health is extremely lucrative. This ecosystem creates risks of harms, from discrimination, to loss of autonomy and dignity, to emotional harms of misplaced targeted ads. The *Dobbs v. Jackson Women’s Health Organization* decision takes an already problematic system into crisis mode, where widespread reproductive health

⁴⁴² *Id.* § 101(b)(A)(i)–(ii).

⁴⁴³ *Id.* § 101(b)(6).

⁴⁴⁴ Edelman, *supra* note 438; Press Release, U.S. Senate Comm. on Com., Sci. & Transp., *supra* note 422.

⁴⁴⁵ Duball, *supra* note 421 (describing debates about federal preemption of state law as “the only contentious stretch during the session”).

⁴⁴⁶ Edelman, *supra* note 438.

⁴⁴⁷ See H.R. 8152 § 404(b)(1)–(4).

⁴⁴⁸ Duball, *supra* note 421 (noting the importance of California’s support for the bill).

data increases risks of harassment, investigation, criminalization, and chilling effects related to a range of pregnancy-related behaviors and outcomes, beyond abortion. Reproductive health across the board is under constant surveillance and an attack on one aspect of reproductive health puts all aspects of reproductive health at risk.

This crisis calls for wholesale and radical changes to the data ecosystem of our country. Although no bill introduced in Congress to date is completely foolproof, a lack of any protections at the federal level is unacceptable—as this Article demonstrates, there is only so much that individual self-management and company goodwill can do. Only with these broad, sweeping changes to data privacy can we hope to move from reproductive health surveillance to meaningful reproductive health privacy.