UC Law Science and Technology Journal

Volume 15 | Number 1 Article 3

2-2024

One Nation, Under Dobbs: How Dobbs v. Jackson Women's Health Impacts Data Privacy for All

Mikayla Domingo

One Nation, Under Dobbs: How *Dobbs v. Jackson Women's Health* Impacts Data Privacy for All

MIKAYLA DOMINGO*

ABSTRACT:

The Supreme Court has gone against the fundamental principle of Stare Decisis in *Dobbs v. Jackson Women's Health Organization,* holding that the constitution confers no right to an abortion. The aftermath of *Dobbs* shines a spotlight on how reproductive and feminine health data are exploited to target women. From geolocation monitoring to abortion clinics, to women's search history and private messages being used in her prosecution, the dystopian prospect of surveillance capitalism is now reality for women in the United States. The immediate impact of Dobbs illuminates the need for greater and clearer data privacy protections have never been more necessary.

However, *Dobbs'* impact will reach far beyond women seeking reproductive health care or abortions. While the aftermath of *Dobbs* has already resulted in an attack on women's data privacy rights, I argue that the complacency with government and private actor's intrusion -largely due to underdeveloped data privacy legal rights- into women's most intimate information will inevitably diminish everyone's data privacy protections over time. Specifically, I argue that the exploitation of such personal data to target women seeking an abortion sets a precedent that will allow countless other groups to have their personal data exploited for whatever their state deems to be a "legitimate government interest." This paper highlights the importance of developing more comprehensive data privacy laws and regulations.

---

* Mikayla Domingo is a Juris Doctor candidate at the University of California, College of the Law, San Francisco. mikayladomingo@uclawsf.edu

Disclaimer: The author acknowledges that all people with a uterus are capable of becoming pregnant, regardless of gender identity. However, for concision and clarity, the term "woman" will be used throughout this article to refer to all people with a uterus and are biologically capable of becoming pregnant.

TABLE OF CONTENTS

INTRODUCTION

Women born in America after 1973 grew up in a society where the prospect of bodily autonomy deprivation by a state law banning abortion is a ghost from the past, laid to rest in *Roe v. Wade*. However, the Supreme Court decision in *Dobbs v. Jackson Women's Health Organization* would revive that haunting piece of history, bringing with it an added curse unique to the digital age. Technology's prevalence in modern society completely changes the privacy landscape from the time before *Roe* was decided. Protected Health Information (PHI) transformed from hand-written physical files, to digitized records subject to the Health Insurance Portability and

Accountability Act (HIPAA)[1] The growing femtech market resulted in booming popularity of fertility and menstruation tracking smartphone apps[2] that women embraced, downloaded, and shared intimate information with. The rise of social media platforms like Facebook connected our personal lives to our friends, but also to third-party apps[3]

Post-*Dobbs*, the data from these various sources would be exploited to target women for purposes ranging from ad targeting[4] to criminal prosecution[5] The *Dobbs* aftermath leaves women disproportionately vulnerable to data privacy violations, but this risk will not stay exclusive to women for long. Over time, the shock value of invasive digital surveillance will plateau into the norm, thereby setting a dangerous precedent for the future. Current case law settles that the Fourth Amendment prevents warrantless government intrusion into cell site location information[6], but what happens when the culprit is a private party, data broker, or third-party app that users did not consent to? These questions are unanswered, and *Dobbs* lays a dangerous foundation for the largely unpaved future of data privacy protections.

In this paper, I argue that unless changes are made at the federal level, state level, and private sector, *Dobbs* has the capacity to deteriorate the progress made in data privacy protections for everyone. This paper begins by discussing the Supreme Court's Decision in *Dobbs v. Jackson Women's Health Organization* in Part I. Part II outlines the current data privacy landscape by demonstrating the progress that has been made thus far in defining privacy harms, while also illuminating the areas that need improvement. Part III illustrates the way women's data has been monetized, weaponized, and remains vulnerable to threats particularly in light of *Dobbs*. Part III further demonstrates how the current data privacy landscape puts the general population's data at risk for privacy invasions, which will only be exacerbated post-*Dobbs*. Finally, Part IV argues that Dobbs has illuminated the necessity

1. *See* Rory Cooksey, *The Use of Technology and HIPAA Compliance,* FORBES (Mar. 12, 2021), https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2021/03/12/the-use-of-technology-and-hipaa-compliance/?sh=defd5581fff4.

2. *See* Anastasia Siapka & Elisabetta Biasin, *Bleeding Data: The Case of Fertility and Menstruation Tracking Apps*, 10 INTERNET POL'Y REV. 1, 2 (Dec. 7, 2021), https://doi.org/10.14763/2021.4.1599.

3. *See generally, In re* Facebook, Inc.,No. 17-17486, (2020) (hereinafter "In Re Facebook").

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

5. Cat Zakrzewski, et. al, *Texts, Web Searches About Abortion Have Been Used to Prosecute Women,* WASH. POST (July 3, 2022), https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/.

6. *See generally*, Carpenter v. United States, 138 S.Ct. 2206, 2217 (2018).

of greater privacy protections and advocates for federal, state, and private sector level change in order to protect data privacy for all.

I. GENERAL OVERVIEW OF *DOBBS* DECISION & IMPACTS

On June 24, 2022, the United States Supreme Court voted 6-3 on an opinion by Justice Alito in *Dobbs v. Jackson Women's Health Organization* that the Constitution does not confer a right to an abortion, thereby overruling *Roe v. Wade* and *Planned Parenthood of Southeastern Pennsylvania v. Casey*[7] The majority found that the right to an abortion is not a fundamental liberty because it is neither "deeply rooted in our history and tradition" nor essential to the nation's "scheme of ordered liberty"[8] On the issue of whether something is a fundamental right, the court engages in historical inquiry into states' common law and ultimately concludes that "until the latter part of the 20th century, there was no support in American law for a constitutional right to obtain an abortion"[9] *Dobbs* leaves it to the states to determine its restrictions on abortion, and lowers the standard of review to rational basis in order to pass constitutional muster[10] Simply, as long as a state legislature can conceive of a rational basis on which the law restricting abortion could serve legitimate state interests, then the law will be upheld[11]

As of February 2023, 13 states have banned abortion, and 5 states have passed laws reducing the gestational limit of viability set in Roe[12] Georgia's Supreme Court granted emergency stay for an injunction, putting a six-week abortion ban into effect[13]; this law was deemed unconstitutional in 2021, but was reinstated post-Dobbs[14] Texas Senate Bill 8 - infamous for its design to shift enforcement from the state to private individuals- also imposes a six-week abortion ban, in addition to creating a $10,000 incentive for private individuals to sue a healthcare worker, abortion provider, or anyone assisting

7. *See Dobbs v. Jackson Women's Health Organization*, SCOTUS BLOG (Aug. 29. 2022), https://www.scotusblog.com/case-files/cases/dobbs-v-jackson-womens-health-organization/.

8. *See* Dobbs, State Health Officer of the Mississippi Department of Health, et. al., v. Jackson Women's Health Organization, et. al., 142 S.Ct. 2228, 2246 (2022).

9. *Id*. at 2235.

10. *Id.* at 2284.

11. *Id.*

12. *See Tracking the States Where Abortion is Now Banned,* N.Y. TIMES (last updated Mar. 23, 2023), https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html.

13. *See Georgia Supreme Court Allows Six-Week Abortion Ban to Again Take Effect*, ACLU (Nov. 23, 2022), https://www.aclu.org/press-releases/georgia-supreme-court-allows-six-week-abortion-ban-again-take-effect

14. *See* N.Y. TIMES, *supra* note 12.

access to an abortion after six weeks[15] As a result, an excited mother-to-be was forced to endure a traumatic and grueling miscarriage for days at home due to uncertainty over the legal ramifications of treatment, when just months prior she had an entirely easier, less painful treatment[16] In Ohio, the "trigger ban" that went into effect would have forced a 10-year-old girl to carry her 27-year-old rapist's child to full term, had she not crossed state lines into Indiana to receive treatment[17] This list does not begin to scratch the surface of the Dobbs decision's impact on women and minor children with childbearing capacities that continues to unfold in the United States.

While the crux of Dobbs focused on the constitutionality of abortion, the language of the decision may raise another question about privacy rights in general. The Constitutional right to privacy is not specifically enumerated in the Constitution, but it was codified in the landmark case of *Griswold v. Connecticut* (1965). When deciding the issue of whether there is an implied right of privacy in a marital relationship, the court reasoned that there are protections within the penumbras of the Bill of Rights that are not specifically enumerated, but nonetheless provide constitutional protections from government interference [18] Further, the Court held that there is a right to privacy in a marital relationship that exists within the "zone of privacy" created by several of these constitutional guarantees and protections[19] Griswold set the precedent for numerous privacy-related cases, including the landmark case of *Roe v. Wade* (1973) which held that the right to privacy encompassed a woman's right to choose whether to have an abortion[20] *Dobbs* departs from precedent founded on a right to privacy. The majority opinion utilized a textualist approach to explicitly reject the notion that there is a constitutional right to abortion because the Fourteenth Amendment's Due Process Clause only protects rights "deeply rooted in the Nation's history" and "implicit in the concept of ordered liberty"[21] The opinion's language raises further concern when it cites a string of privacy-related cases that are not "deeply rooted

15. *See Texas Abortion Ban Takes Effect, Ending Almost All Abortion Care in the State,* CTR. FOR REPROD. RTS. (Sept. 1,2021), https://reproductiverights.org/texas-abortion-ban-sb8-takes-effect/.

16. *See* THE DAILY, *How Abortion Bans are Restricting Miscarriage Care,* N.Y. TIMES, at 3:45-9:18 (July 20, 2022), https://www.nytimes.com/2022/07/20/podcasts/the-daily/abortion-roe-miscarriage-treatment.html.

17. *See* Sarah McCammon & Becky Sullivan, *Indiana Doctor Says She Has Been Harassed for Giving an Abortion to a 10-Year-Old,* NPR (July 26, 2022), https://www.npr.org/2022/07/26/1113577718/indiana-doctor-abortion-ohio-10-year-old.

18. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

19. *Id.* at 485.

20. *See* Roe v. Wade, 410 U.S. 113, 152-64 (1973).

21. *See* Caitlin Chin, *What Privacy in the United States Could Look Like Without Roe v. Wade*, CTR. FOR STRATEGIC & INT'L. STUD. (May 25, 2022), https://www.csis.org/analysis/what-privacy-united-states-could-look-without-roe-v-wade.

in history," including *Griswold v. Connecticut* 381 U.S. 479 (1965), *Loving v. Virginia*, 388 U.S. 1 (1967), *Lawrence v. Texas* 539 U.S. 558 (2003), *Obergefell v. Hodges*, 576 U.S. 644 (2015), and many more[22] Further, the overturning of a firmly-established right, coupled with the hint at other privacy cases established through the same logic to find a fundamental right raises serious questions and concerns for the future of privacy as we know it. Specific to this paper, the Dobbs decision has the potential to adversely impact all of the progress made with regard to data privacy rights.

II. THE DATA PRIVACY LANDSCAPE

Laws governing data privacy in the United states are analogous to a patchwork blanket: various types of law govern privacy, ranging from contracts, to torts, to statutory law[23] Federal statutory law is governed by different agencies, with various federal agencies providing private rights of action[24] and setting national standards[25] State laws are also a source for private rights of action, with few establishing consumer privacy protections[26] The data privacy landscape is perpetually evolving to keep pace with technological transformations. Pre-*Dobbs*, privacy law has steadily advanced and adapted to modern-era consumer needs related to technology's growing prevalence in society. However, the post-*Dobbs* aftermath brings the deficits in the current data privacy framework to the forefront, and highlights the need for more comprehensive data privacy protections.

A. Advances in data privacy protections

1. *Standing for Intangible Harms: Disclosing Sensitive Private Information*

Pre-*Dobbs*, Federal courts have steadily recognized privacy harms as actual harms.Privacy law in the United States requires showing harm as an element in establishing a cause of action[27] Historically, the requirement to establish harm had functioned as a gatekeeper to Article III standing[28] in

22. *See* 142 S.Ct. at 2257-58.

23. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms,*102 B. U. L. REV. 793, 796 (2022), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.

24. *See Id.,* at 810 (explaining the Telephone Consumer Protection Act ("TCPA") to address privacy with respect to telemarketing, or the Fair Credit Reporting Act ("FCRA") to protect information collected by consumer reporting agencies).

25. *See, Infra* Section III. part 4.

26. *See* Citron & Solove, *supra* note 23, at 811.

27. *Id.* at 796.

28. *See* Spokeo v. Robins, 578 U.S. 330, 339-41 (2016) (explaining a plaintiff must have Article III standing to bring a case to federal court, which requires a plaintiff to establish that he or she suffered an injury in fact that is "concrete" and "particularized." An injury is concrete if it

privacy cases[29] However, the Northern District Court of California took a momentous step in recognizing intangible data privacy harms as actual harms[30] The District Court held that Facebook's widespread disclosure of user's sensitive and private information to third party app was concrete and particularized to the class action plaintiffs, sufficient to confer article III standing[31] The District Court noted that other courts agree that disclosing sensitive private information, even without further consequences, is a type of intangible injury that has given rise to Article III standing[32] There is now precedent that data privacy harms constitute actual injuries sufficient to confer Article III standing. The recognition of data privacy invasions as inflicting actual injury affirms the "importance of privacy in our society"[33]

2. *Internet tracking- Cookies and the Wiretap Act*

Federal courts are beginning to find that companies are not a "party to a communication," subjecting them to liability under the Wiretap Act. The Wiretap Act (1934) prohibits the unauthorized interception and disclosure of wire, oral, and electronic communications[34], and has been extended to provide a private right of action through the Electronic Communications Privacy Act ("ECPA")[35] The Wiretap Act contains a liability carveout for anyone considered "a party to the communication"[36] that companies like Facebook and Google claim to qualify under to establish a defense [37] Wiretap Act litigation commonly pertains to the use of "cookies" by companies that track

actually exists, but is not required to be tangible. For an injury to be "particularized," it must personally and individually affect the plaintiff).

29. *See* Keats Citron & Solove, *supra* note 23, at 800-01.

30. *See* In Re Facebook, Inc., Consumer Privacy User Profile Litigation, Pretrial Order No. 20: Granting in Part and Denying in Part Motion to Dismiss First Amended Complaint, MDL No. 2843 at 14 (recognizing the dissemination of plaintiff's sensitive information to third parties as a violation of privacy, sufficient to confer standing).

31. *Id.*

32. *Id.*

33. *Id.* at 16.

34. *See* 18 U.S.C. §2511.

35. *See Electronic Communications Privacy Act (ECPA)*, ELEC. INFO. PRIV. CTR., https://epic.org/ecpa/ (last visted on Sept. 24, 2023).

36. Note that the Wiretap Act fails to define the term "party" to a communication, which has resulted in differing interpretations in circuit courts, leading to circuit splits in the Wiretap Act's application.

37. *See* Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online,* 29 WASH. & LEE J. CIV. RTS. & SOC. JUST. 187, 194, (2022), https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1541&context=crsj.

user's activity across the internet[38] Cookies[39] are small text files stored on a user's device browser whenever they visit a website[40] The (relatively) early case of *In Re DoubleClick Inc Privacy Litigation* set the tone for subsequent Wiretap Act cases related to cookies. The United States District Court of the Southern District of New York ruled that a company does not violate the ECPA by storing and accessing cookies on an internet user's harddrive[41] The District Court found that the ECPA's "party to a communication" exception applied because affiliated websites could authorize DobleClick's access to internet communications[42] However, some circuit courts are departing from this holding. In the Ninth Circuit, Facebook recently settled for $90 million upon the court's finding that plaintiffs had sufficiently alleged violations of the wiretap Act and the California Invasion of Privacy Act (CIPA)[43]

3. *4th Amendment - Geolocation Tracking*

Supreme Court jurisprudence has also revamped Fourth Amendment protections in order to address the "seismic shifts in digital technology."[44] The Fourth Amendment of the United States Constitution protects against unreasonable searches and seizures from the government without a warrant[45] The Fourth Amendment is violated when the government's warrantless search violates a person's "reasonable expectation of privacy."[46] The Court addressed the invasiveness of warrantless geolocation searches captured

38. *See generally* In Re Facebook, supra note 3 at 7-8 (exemplifying a current case where cookies use, collection, and storage of user's information was crucial to the issue of data privacy litigation); *see also* Brown v. Google, LLC, No. 20-cv-3664-YGR, 2022 WL 17961497, at *10 (N.D. Cal. Dec. 12, 2022).

39. *See What is Online Tracking and How Do Websites Track You?* KOOFR BLOG, https://koofr.eu/blog/posts/what-is-online-tracking-and-how-do-websites-track-you (last visited on Sept. 24, 2023).

First party cookies are created by the website's owner and are used to improve a user's boring experience, and help the website operate basic functions. By contrast, third party cookies are created by other entities to track users across the internet and store browsing history across multiple websites for long periods.

40. *See Id.*

41. *See* In Re DoubleClick Inc. Privacy Litigation 154 F. Supp 2d 497, 502-03 (2001).

42. *Id.* at 514 (finding that the DoubleClick-affiliated websites were "parties to the communication[s]" because plaintiffs had given DoubleClick sufficient consent to intercept them).

43. *See* Allison Grande, *Facebook to Pay $90M to Settle Suit Over Tracking Users*, LAW360 (Feb. 15, 2022), https://www.law360.com/classaction/articles/1465215/facebook-to-pay-90m-to-settle-suit-over-tracking-users.

44. 138 S.Ct. at 2219.

45. U.S. CONST. amend. IV.

46. A person has a reasonable expectation of privacy where the individual exhibits both a subjective expectation of privacy in the place or thing being searched, and that subjective expectation of privacy is objectively reasonable. *See* Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring).

through Cell Site Location Information (CSLI) in *Carpenter v. United States*, (2018). *Carpenter* held that a person has a "legitimate expectation of privacy in the record of his physical movements as captured through CSLI" and therefore the warrantless acquisition of CSLI was a search within the meaning of the fourth amendment[47] In its decision, the Court emphasized the pervasive role that cell phones play in daily life, as "indispensable to participation in modern society."[48]The third party doctrine does not apply to the unique nature of CSLI, because the transmitted location information is not truly "shared" by the user. Phones, by nature of their operation, log cell site records without any action on the user's end[49] Importantly, CSLI was distinguished from traditional methods of geolocation tracking such as GPS data based on the time-stamped data's ability to "provide an intimate window into a person's life," and its ability to retroactively collect historical data from any period at practically no expense[50] Furthermore, *Carpenter v. United States* represents a consequential move in favor of protecting sensitive data from warrantless, "near-perfect surveillance" by the government in the digital age[51] *Carpenter* demonstrates the Supreme Court's awareness of technology's capability to interfere with Americans' constitutional rights in the digital age, if left unchecked.

B. Shortcomings in the Current Landscape

1. *The Current Statutory Protections are Insufficient to Adequately Protect Data Privacy*

US Privacy law is not cohesive. There is no singular comprehensive federal privacy law that regulates all types of data, but rather a "sprawling patchwork" of various bodies of law and statutes.[52] Privacy lawyers must dig for a cause of action or remedy in a sea of acronyms such as HIPAA, ECPA, FCRA, or the FTC Act that target specific types of data in specific circumstances.[53] The current federal framework is too narrowly focused to provide

47. *Id*. at 2217.

48. *Id.* at 2210.

49. *Id.* at 2220-21.

50. *Id.* at 2217-18.

51. *See* Nathan Freed Wessler, *The Supreme Court's Most Consequential Ruling For Privacy in the Digital Age, One Year In*, ACLU (June 18, 2019), https://www.aclu.org/news/privacy-technology/supreme-courts-most-consequential-ruling-privacy-digital.

52. *See* Citron & Solove, *supra* note 23 at 796.

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

meaningful protections for consumers.[54] Even if a privacy harm categorically fits under one of these highly-specialized statutes, Supreme Court precedent from Spokeo a "bare procedural violation" may be insufficient to confer standing because "not all procedural violations create harm or material risk of harm."[55]

Additionally, the US enforcement mechanism is remedial rather than preventative.[56] For example, the FTC enforces online privacy, but the agency cannot stop wrongdoing unless the company breaches its own privacy policy.[57] Because most privacy harms involve future uses of data and thereby present a wide range of future harms, the current legal framework is unequipped to uniformly address future risks of harm from privacy violations.[58] In fact, the current weight of authority leaning against finding harm for future privacy harms.[59]

2. *No Meaningful Restrictions on Databrokers*

The lack of regulation in the data broker industry not only fails to protect consumers from data privacy invasions, but also financially incentivizes the proliferation of mass data collection.[60] Data Brokers are companies that collect and aggregate multitudes of personal information, purchase history, health information, browsing history, and even real-time location data in order to algorithmically generate user profiles for profit.[61] These aggregated data profiles are sold to marketing companies that subsequently use this information to target consumers based on the "bucket" they fall into.[62] Personal data is commodified and approached through a market-based lens,

54. *See* Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix it,* 42 J. CORP. L. 461, 466 (2016), https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jcorl42&id=479&men_tab=srchresults.

55. *See* Robins v. Spokeo, Inc. 131 HARV. L. REV. 894, 896 (explaining the Supreme Court's reasoning in Spokeo, Inc. v. Robins), https://harvardlawreview.org/2018/01/robins-v-spokeo-inc/.

56. *See* Fairclough, *supra* note 54 at 467-68 (illustrating how U.S. enforcement of privacy laws requires an individual's private information to be misused and meet several elements before a federal agency can provide narrow relief to limited circumstances, rather than requiring greater protection on the front end).

57. *Id.* at 467.

58. *See* Citron & Solove, *supra* note 23 at 817.

59. *Id.* at 817, 835.

60. *See Data Brokers*, ELEC. INFO. PRIV. CTR., https://epic.org/issues/consumer-privacy/data-brokers/ (last viewed Apr. 5, 2023).

61. *Id.*

62. *See* Ashley Kuempel, *The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry,* 36 NORTHWESTERN J. OF INT'L. L. & BUS. 207, 210, 220 (2016), https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/nwjilb36&id=214&men_tab=srchresults.

employing the rationale that companies have a legitimate business interest in acquiring personal information that should not be restricted by privacy concerns.[63] Rather than treating data privacy as a right to be protected,[64] the current U.S. legal landscape allows individual privacy interests to fall second to business interests.[65]

Because the data broker industry is unregulated by federal statutory laws, the ball remains in data brokers' court to "self-regulate" their privacy standards based on the industry norms.[66] This effectively meaningless standard does nothing to dissuade data brokers from continuously collecting, selling, commodifying, and exploiting users' personal data. Since consumers are largely unaware of data brokers existence and the detailed, sensitive information they collect[67], the current framework disincentivizes transparency with consumers about these companies' data collection practices and purposes.[68] The lack of awareness and transparency prevents consumers from seeking or receiving redress.[69]

3. *Remedies are Insufficient to Provide Meaningful Redress*

There is a misalignment between enforcement goals and remedies in privacy law.[70] When the goals of enforcement are not aligned with the appropriate remedy, the law suffers.[71] Privacy law has three predominant goals: (1) compensation, (2) deterrence, and (3) equity.[72] However, the law is too rigidly formalistic to redress the various forms of privacy harms when harm remains the crux of the analysis.[73] Where restitution is a remedy, judges must first determine whether the defendant can return what it took from the plaintiff; if not, the court must assign a value to the degree of enrichment.[74]

63. *See id.* at 215.

64. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (defining privacy rights as the right "to be let alone").

65. See Kuempel, *supra* note 62, at 215.

66. *See id.* at 216.

67. *See* Edith Ramirez, et. al., *Data Brokers: A Call for Transparency and Accountability,* FEDERAL TRADE COMMISSION (May 2014) at C-3 (Concurring statement of Commissioner Julie Brill at app. C-1).

68. *See* Kuempel, *supra* note 62 at 218-19.

69. *See id.* at 221-22.

70. *See* Citron & Solove, *supra* note 23 at 819.

71. *Id*. at 820.

72. *Id*. at 819.

73. *Id*. at 825.

74. *See* Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 673 (2019), https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/indana94&id=701&men_tab=srchresults.

However, value is most frequently equated with monetary relief,[75] which may be inadequate to remedy emotional distress caused by a privacy violation, for instance. Emotional distress is one of the most common harms from privacy violations, yet the body of case law recognizing emotions distress as cognizable harm is inconsistent.[76] Therefore, plaintiffs seeking redress for emotional harm caused by a privacy invasion may only find redress within the narrow confines of a federal statute's private right of action, thus misrepresenting their grievances and setting precedent for others in the same situation.

Even if a plaintiff passes the high hurdle of establishing harm, the form of relief provided may also be insufficient to provide meaningful redress. Take class action suits, for example. Class action suits are commonly used in privacy litigation due to the massive costs of bringing suit.[77] In many cases, privacy harms are small but numerous, thereby involving aggregation of multiple small harms to multiple individuals.[78] While the hope is that harm aggregation in a class action will address a large scale problem and have a societal impact, class actions are an imperfect vehicle.[79] Class actions are costly, time-consuming, and plaintiffs lack control over the lawsuit, which often results in settlement that enhance class counsel's payout.[80] Even in the event of settlement, cash payout is miniscule to each class member relative to the harm suffered.[81]

III. *DOBBS* IMPACT ON DATA PRIVACY RIGHTS

A. For Women's Reproductive Health Data

Dobbs has illuminated the concerns surrounding and prevalence ofsurveillance capitalism.[82] In light of *Dobbs*, privacy attorneys urge that "once a

75. See *id.* at 673 (listing possible monetary measures for enrichment, demonstrating how remedies are most likely provided in the form of financial compensation).

76. *See* Citron & Solove, *supra* note 23 at 841.

77. *See* Eric Goldman, *The Irony of Privacy Class Action Litigation,* 10 J. ON TELECOMM & HIGH TECH L. 309, 309, 317 (2012), https://digitalcommons.law.scu.edu/facpubs/597.

78. Citron & Solove, *supra* note 23, at 816.

79. *Id.* at 816–17.

80. Goldman, *supra* note 77, at 314–16.

81. In the largest settlement ever recovered in the US for a data privacy class action, Facebook was ordered to pay $725 million to the Settlement Class. However, the enormous class size resulted in a payout of approximately $2.50 - $2.90 per class member. Plaintiff's Notice of Motion and Motion to Certify a Settlement Class and Grant Preliminary Settlement Approval at 12, *See In re* Facebook Consumer Privacy User Profile Litigation, Dkt. No. 18-md-02843 (N.D. Cal. Jun 06, 2018), ECF No. 1096.

82. *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospect of and Information Civilization,* 30 J. INFO. TECH. 75, (2015), https://journals.sagepub.com/doi/pdf/10.1057/jit.2015.5 (coining the term "surveillance capitalism."

tech company knows where you've been, what you've Googled, and even know how your fingerprints look, you're incredibly vulnerable if that data gets into the wrong hands."[83] This segment of the paper focuses on the types of private data that, if in the wrong hands, would have detrimental impacts on women in the aftermath of Dobbs.

1. *FemTech & Surveillance Capitalism*

Dobbs raises concern for health data stored in femtech.[84] Femtech[85] is marketed as helpful for tracking women's health, menstruation, and fertility. Yet at its core, femtech companies are in the business of data extraction. For these apps to fulfill their purpose, the apps collect deeply personal information, such as a woman's age, the type of birth control she takes, her sexual activity, and stages of pregnancy.[86] Because most period tracker apps are free, these companies earn their profits by selling user data to third party advertisers, and "other industries in assessing women."[87] This data is nearly impossible to erase.[88] As a result, nearly all femtech apps expose users to privacy and security risks through data collection and subsequent use by third parties.[89] This business model is a recipe for disaster that became reality in an FTC lawsuit against period and fertility tracker app Flo. In 2021, Flo settled FTC allegations that the company misled app users about disclosing their health data when it shared personal information with outside data analytics providers, despite promising to maintain data privacy and only use it

Surveillance Capitalism "unilaterally claims human experience as free raw material for translation into behavioral data" and creates "prediction products'' that will anticipate what a person does now, soon, and later).

83. *See* Jay Edelson, *Post-Dobbs, Your Private Data Will Be Used Against You*, BLOOMBERG L. (Sept. 22, 2022), https://news.bloomberglaw.com/us-law-week/post-dobbs-your-private-data-will-be-used-against-you [https://perma.cc/F8AT-TDTF].

84. *See* Laura Travis, *ANALYSIS: Who Will Regulate Femtech After Dobbs?*, BLOOMBERG L. (Nov. 13, 2022), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-who-will-regulate-privacy-in-femtech-after-dobbs.

85. *See Femtech,* CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/femtech [https://perma.cc/W97J-VZSU] (defining Femtech as "technology related to a woman's health, for example, software that records information about menstruation … and fertility").

86. *See* Julia Logue, *Users of Femtech Should be Concerned - In a Post-Dobbs World, Their Personal Data Could be Used Against Them*, GEO. L. REV. (Nov. 2022), https://georgetownlaw-techreview.org/users-of-femtech-should-be-concerned-in-a-post-dobbs-world-their-personal-data-could-be-used-against-them/GLTR-11-2022/ [https://perma.cc/FA7V-D3SQ].

87. Michele Estrin Gilman, *Periods for Profit and the Rise of Menstrual Surveillance*, 41 COLUM. J. GENDER & L. 100, 102 (2021), https://journals.library.columbia.edu/index.php/cjgl/article/view/8824/4562.

88. *Id*. at 100.

89. *See* Leah R. Fowler & Michael R. Ulrich, *Femtechdystopia,* 75 STAN. L. REV. 1233, 1266 (June 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4099764.

for apps services.[90] According to the Complaint, Flo disclosed sensitive health data from millions of its users, including a user's pregnancy, to third parties such as Facebook and Google's analytics divisions, with no limits on how these third parties could use this health data.[91]

The consequences of women's data stored in their femtech apps are far more dire in the post-*Dobbs* landscape. Period and fertility trackers possess uniquely intimate data because the technology is specifically designed to meet menstrual and reproductive health needs.[92] When aggregated, this data clearly reveals whether a woman has had an abortion, and can be used to prosecute her.[93] In a state where abortion is criminalized, government agents could turn to a period tracker app to determine a woman's last menstrual date, to determine gestational age, or identify suspicious patterns identifying failed abortions.[94] The lack of privacy and security regulations for femtech allow the law enforcement to access this deeply personal information without a warrant by purchasing this data directly from femtech companies, or from one of the many third parties that have access to it.[95] Alternatively, consider Texas S.B. 8's private actor incentive to enforce the anti-abortion law: a non-government actor could purchase this data from a company or a databroker, provide evidence of a likely abortion[96] to law enforcement, and also collect on the $10,000 for bringing a civil suit. Femtech companies' troves of personal data, which can all to easily be exploited in the wrong hands under the current privacy landscape, with the only protection stemming from companies "self regulation."[97]

2. *Internet Tracking and Surveillance Capitalism*

A woman's internet search history related to her reproductive health can be used as evidence of criminal intent in states where abortion is

90. See FTC, *supra* note 4.

91. *See* Rina Torchinsky, *How period tracking apps and data privacy fit into a post-Roe v. Wade climate,* NPR (June 24, 2022), https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps [https://perma.cc/4HG4-7BBG].

92. *See* Fowler & Ulrich, *supra* note 89, at 1261, 1266.

93. *See* Logue, *supra* note 86.

94. *See* Fowler & Ulrich, *supra* note 89, at 1237.

95. *See* Logue, *supra* note 86.

96. *See* Yasmeen Abutaleb & Emily Wax-Thibodeaux, *Missouri Reviewed Data About Planned Parenthood's Patients, Including Their Periods, to Identify Failed Abortions,* WASH. POST (Oct. 30, 2019), https://www.washingtonpost.com/health/missouri-trackedplanned-parenthood-patients-periods-in-spreadsheet-top-health-officialsays/2019/10/30/e96791d0-fb42-11e9-ac8c-8eced29ca6ef_story (describing how a Missouri state health director monitored and reviewed women's menstrual dates in order to investigate "failed abortions," thus demonstrating the importance of menstrual information in enforcing abortion restrictions).

97. *See* Gilman, *supra* note 87 at 105, 109-11.

criminalized.[98] While fertility apps and FemTech are ripe for abuse, police have already turned to direct messages on social media,[99] text messages, and search histories on mobile devices and computers.[100]

Americans seek medical advice online at increasing rates. The majority of the population (68.9%) turns to the internet first to search for health or medical information.[101] A decade-long study revealed that across survey years, women under 50 years old are the largest population that seek health and medical information.[102] Young women in particular turn to the internet for information about safe and accessible abortion options, sometimes outside of a clinic setting.[103] Another study[104] found that majority of its participants who were pregnant and did not want to be had searched terms like "self abortion" due to uncertainty an accessible healthcare facility that provided abortions, while one-quarter were unsure if abortion was legal in her state.[105] Women prefer to use the internet to resolve the deeply personal issue of an unwanted pregnancy because of lower costs, lack of mobility, barriers to care, but mostly because women wanted more privacy.[106] However, internet searches are anything but private. Willingness to engage with internet services have resulted in an increased reliance on a system that collects, stores, sells, and effectively exploits people's online activity.[107]

Web searches can be used by law enforcement to provide evidence of intent for a prosecutor to indict a woman of violating a state abortion-restriction law. In 2017, Latice Fisher's web search history, which included searches for how to induce a miscarriage and proof of her misoprostol purchase, was use as evidence of her criminal intent in a grand jury proceeding

98. *See* Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary,* 50 U. BALT. L. REV. 1, 5 (2020), https://scholarworks.law.ubalt.edu/ublr/vol50/iss1/2/.

99. *See* Emily Baker-White & Sarah Emerson,

Facebook Gave Nebraska Cops A Teen's DMs. They Used Them To Prosecute Her For Having An Abortion, FORBES (Aug. 8, 2022), https://www.forbes.com/sites/emilybaker-white/2022/08/08/facebook-abortion-teen-dms/?sh=e2f2101579c1.

100. *See* Zakrzewski, et. al., s*upra* note 5.

101. *See* Lila J. Finney Rutten et. al., *Online Health Information Seeking Among US Adults: Measuring Progress Toward a Healthy People 2020 Objective,* 134 PUB. HEALTH REP. 617, 619 (2019), https://doi.org/10.1177/0033354919874074.

102. *Id.*

103. *See* Jenna Jerman et. al., *What are people looking for when they Google "self-abortion"?,* PUBMED CENT. (June 5, 2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5988356/.

104. *See id.* (describing a 2017 study's methodology involved administering a survey in response to user's interaction with a targeted ad that appeared when users searched one of 26 key search terms that the study anticipated to be Googled in inquiring on self abortion).

105. *Id.*

106. *See* Conti-Cook, *supra* note 98, at 24.

107. *See id.* at 28.

where Fisher was eventually indicted for second degree murder.[108] Following *Dobbs*, states that have criminalized abortion will increasingly rely on digital footprints through aggregating women's femtech information,[109] search histories, and geolocation.[110]

Additionally, an investigation by Time into crisis pregnancy centers (CPCs)[111] revealed that these centers collect vast amounts of sensitive personal data that legal experts say pose a privacy risk in the wake of more states criminalizing abortion.[112] Because CPCs are not licensed medical facilities and are not bound by federal privacy laws, they can share client information with other organizations.[113] As a result of the lack of secured privacy, highly sensitive data from CPC websites have been shared with Facebook.[114] An investigation by Reveal and The Markup analyzed the websites of nearly 2,500 CPCs, and found that at least 294 shared extremely sensitive visitor information, including whether a woman was considering abortion.[115] CPCs and other businesses have discretion in choosing to instal the Meta Pixel[116] to deliver targeted advertising in order to deter a woman from having an abortion.[117] In sum, a person's web activity can be weaponized by law

108. *Id.* at 3-5.

109. *See* discussion *supra* part III.A.1.

110. *See* discussion *infra* Part III.A.3.

111. *See Issue Brief: Crisis Pregnancy Centers*, AM. CONG. OF OBSTETRICIANS AND GYNECOLOGISTS (Oct. 2022), https://www.acog.org/-/media/project/acog/acogorg/files/advocacy/cpc-issue-brief.pdf (Crisis pregnancy centers are "facilities that represent themselves as legitimate reproductive health care clinics providing care for pregnant people but actually aim to dissuade people from accessing certain types of reproductive health care, including abortion care and even contraceptive options. Staff members at these unregulated and often nonmedical facilities have no legal obligation to provide pregnant people with accurate information and are not subject to HIPAA or required by law to maintain client confidentiality . . . CPC staff members can divert patients from accessing comprehensive medical care and information by positioning the facility as a legitimate health care clinic even though it doesn't actually offer the full range of reproductive health care. By using deception, delay tactics, and disinformation, CPC staffs undermine the tenets of informed consent and patient autonomy and impede access to comprehensive, ethical care").

112. *See* Abigail Abrams, *Exclusive: Elizabeth Warren and Senate Democrats Press Crisis Pregnancy Centers on Abortion Data Gathering,* TIME (Sept. 21, 2022), https://time.com/6214503/elizabeth-warren-crisis-pregnancy-centers-abortion-data/.

113. *Id.*

114. *See* Gracie Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients,* REVEAL (June 15, 2022), https://reveal-news.org/article/facebook-data-abortion-crisis-pregnancy-center/.

115. *Id.*

116. *See Meta Pixel,* META, https://developers.facebook.com/docs/meta-pixel/ (last visited Sept. 23, 2023) (defining the Meta Pixel as "a snippet of JavaScript code that allows you to track visitor activity on your website. Tracked activities appear in the Ads Manager where they can be used to "measure the effectiveness of your ads, to define custom audiences for ad targeting, for Advantage+ catalog ads campaigns, and to analyze that effectiveness of your website's conversion funnels").

117. *Id.*

enforcement, as well as utilized to target a woman through targeted ads to undermine her autonomy in managing her pregnancy.

3. *Geolocation Tracking*

Post-*Dobbs*, Geolocation data can be weaponized against women seeking reproductive healthcare. There is an increasing likelihood that states may turn to location data for evidence to prosecute women seeking an abortion in a state with an abortion ban. *Carpenter* demonstrates that data, especially in the aggregate, can reveal a plethora of data about an individual.[118] Geolocation data is the type of observed data from which information about health data can be inferred.[119] States criminalizing abortion have demonstrated an increasing reliance on location data, particularly through geofence warrants.[120] For example, Google is one of the most prolific location data collectors, and had received 5,864 geofence warrants between 2018 through 2020 from 10 states that have criminalized abortion as of June 5, 2022.[121] Geofence warrants will be a "uniquely dangerous" tool in states with abortion bans, for its widespread use can quickly be weaponized to identify women who have visited a reproductive health facility, and perhaps use this information to prosecute her.[122]

Additionally, individuals or groups can purchase such data without a warrant through data brokers. In its complaint against Kochava, a databroker, the FTC alleges that the company carelessly sold geolocation data from hundreds of millions of mobile devices, allowing purchasers to track people at sensitive locations, including reproductive health clinics.[123] Such information could also be used to identify medical professionals who perform or assist in performing abortion services.[124] In another instance, data broker Copley Advertising provided geofencing technology to an Evangelical Christian organization to harass women at abortion clinics through running anti-abortion ads, among some titled "You Have Choices" and "You're Not

118. *See generally*, Carpenter v. United States, 138 S. Ct. 2206 (2018).

119. *See* Anya E. R. Prince, *Location as Health,* 21 HOUS. J. HEALTH L. & POL'Y 43, 52 (2021), https://houstonhealthlaw.scholasticahq.com/article/31661-location-as-health.

120. *See Geofence Warrants and the Fourth Amendment,* 134 HARV. L. REV. 2508, 2509-10 (2021), https://harvardlawreview.org/2021/05/geofence-warrants-and-the-fourth-amendment/ (describing Geofence warrants are one of many tools employed by law enforcement when the identity of a suspect is unknown, but law enforcement specifies a location and time period for private companies to produce a list of cellphones and affiliated users from their location databases who were at or near the specified area at the specified time).

121. 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.

122. *Id.*

123. *See* FTC, *supra* note 4.

124. *Id.*

Alone." [125] Through this technology, Copley would "tag" smartphones or internet enabled devices that enters or exits an abortion clinic by using any information stored, transmitted or received by the device, including but not limited to GPS, IP address, Bluetooth technology, or device identification information.[126] These recent cases exemplify data broker's unbridled capacity to exploit women's health data for capital gain, while subjecting women to coercive advertising, intimidation, and interference with her bodily autonomy.[127]

Carpenter foresaw the dangers of unbridled geolocation tracking as technology perpetually advances, and Dobbs is a real-time demonstration of how the lack of surveillance protections against non-government entities inflict actual harm on women.

4. *HIPAA*

While users of femtech or social media made the decision to share information on a digital platform (albeit they did not always consent to the use of that data by third parties), the digitization of their protected health information (PHI) is usually the work of their healthcare providers. Cloud technology helped health care providers manage their increasing caseloads in terms of storage, communications, convenience, and analysis of PHI.[128] However, *Dobbs* shines a spotlight on how this convenience creates serious privacy concerns,[129] especially for women seeking reproductive healthcare in states with abortion bans.[130]

HIPAA is a federal law that requires covered entities, such as healthcare providers, health plans, and business associates, to protect personal health information from disclosure without the patient's knowledge or consent.[131] Additionally, HIPAA's Privacy Rule establishes requirements for the use

125. Justin Sherman, *The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics,* LAWFARE (Sept. 19, 2022), https://www.lawfareblog.com/data-broker-caught-running-anti-abortion-ads%E2%80%94-people-sitting-clinics.

126. *Id.*

127. *Id.*

128. Joyce L.T. Chang, *The Dark Cloud of Convenience: How the New HIPAA Omnibus Rules Fail to Protect Electronic Personal Health Information* 30 LOY. OF L.A. ENT. L. REV. 119, 120 https://heinonline-org.uclawsf.idm.oclc.org/HOL/Page?collection=journals&handle=hein.journals/laent34&id=134&men_tab=srchresults.

129. *Id.* at 122.

130. *See* Ellen Wright Clayton & Peter J Embí, et. al., *Dobbs and the future of health data privacy for patients and healthcare organizations,* 30 J. AM. MED. INFORMATICS ASS'N 155, 157 https://academic.oup.com/jamia/article/30/1/155/6680473.

131. *See Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CDC, https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

and disclosure of PHI by covered entities, reiterating that "regulated entities can use or disclose PHI, without an individuals signed authorization, only as expressly permitted or required by the Privacy Rule" or where the purpose of disclosure is narrowly tailored to protect the individual's privacy.[132] Thus, where a law requires disclosure of an individual's PHI, the Privacy Rule says covered entities are permitted, but not required to disclose the PHI.[133]

However, HIPAA's protections are exclusive to covered entities and PHI, meaning the administrative and technical safeguards provided by HIPAA would not shield the highly-personal data collected by femtech apps.[134] For example, HIPAA would not stop most Femtech companies from sharing user's data with third parties.[135] Because the company is not a covered entity and despite the personal nature of fertility information, the fact that it is not PHI puts this data outside of HIPAA's scope of protections.[136] HIPAA also does not protect inferences that can be made about health through aggregated data collected by companies, such as location data.[137] Cell phones ubiquitously collect GPS location data which companies can use to create a "diary on [ones] every movement."[138] This digital map would reveal whether a woman visited a clinic, or when she stopped by a pharmacy to pick up a prescription for mifepristone to infer that she had induced an abortion, and could be used as evidence against her in a criminal prosecution.

In conclusion, modern reliance on technology illustrates how fundamentally different the world is compared to when *Roe v. Wade* was decided. As a result of the ever-changing digital landscape, there are seemingly endless routes of digital trailers for law enforcement to investigate, whether it be through a woman's personal search history, to her information on her period tracker app, to her actual physical location that is constantly tracked, logged, and stored by her mobile device.

132. *See Privacy of Health Information Post-Dobbs and OCR Guidance on the Protections Afforded under HIPAA*, ROPES & GRAY (July 21, 2022), https://www.ropesgray.com/en/newsroom/alerts/2022/july/privacy-of-health-information-post-dobbs-and-ocr-guidance-on-the-protections-afforded-under-hipaa (Hereinafter "Ropes and Gray").

133. *See* Clayton et. al., *supra* note 130, at 155. *See also* Ropes and Gray.

134. *See* Fowler & Ulrich, *supra* note 89, at 48-49.

135. *Id.*

136. *See* Travis, *supra* note 84.

137. *See* Prince, *supra* note 119 at 52-53 (defining inferred data, and providing examples of its function).

138. Stuart A. Thompson & Charlie Warze, *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.

B. For the General Population

Dobbs has illuminated the threat to women's data privacy in regards to their reproductive information, as well as the lack of recourse to remedy or protect such intrusions. However, these data privacy intrusions will not only impact women. *Dobbs* reinforces the value of privacy in our society, and the detriments of losing it.[139] In the big tech era, internet user's lives are inundated by commercial surveillance through data brokers, cookie tracking, and infinite other invasions that fly under the average consumer's radar. This section highlights a few ways that *Dobbs* impacts on women parallels ongoing privacy invasions impacting more general categories of Americans.

1. *Geolocation Tracking*

Much like geolocation tracking jeopardizes the privacy of women attending abortion clinics, it similarly jeopardizes the First Amendment rights of all individuals who carry a mobile device.[140] As previously discussed, "Geofencing" or "reverse-locating" is a tool employed by law enforcement in asking companies to "sweep search" a location for user's data when an individual's identity is unknown.[141] Geofencing has been used to identify individuals attending a protest. After the infamous murder of George Floyd by a police officer in 2020 sparked protest across the nation, federal investigators quickly "geofenced" arson areas across Kenosha and demanded Google provide information on all devices across those sites.[142] The overbroad scope of these geofence warrants captured data from innocent residents and protesters not involved in the arson, and provided that information to the federal government.[143] While abortion has lost its status as a constitutional right, the freedom of assembly is an enumerated first amendment right that is fundamental to a functioning democracy. The chilling effects that extensive location surveillance will have on exercising that right is a threat to democracy that must be curbed by heightened data privacy protections. That

139. *See* Edelson, *supra* note 83.

140. *See* Thompson & Warze, *supra* note 138 (The Times Privacy Project obtained and reviewed a company's data file containing the logged movements through 50 billion location bings from the mobile phones of over 12 million Americans in several major cities, demonstrating how each piece of information is used to reveal the precise location of a single smartphone over months, creating a "diary of your every movement").

141. Note, *Geofence Warrants and the Fourth Amendment,* 134 HARV. L. REV. 2508, (2021), https://harvardlawreview.org/2021/05/geofence-warrants-and-the-fourth-amendment/ [hereinafter, "note"].

142. *See* Thomas Brewster, *Google Dragnets Harvested Phone Data Across 13 Kenosha Protest Acts of Arson,* FORBES (Aug. 31, 2021), https://www.forbes.com/sites/thomasbrewster/2021/08/31/google-dragnets-on-phone-data-across-13-kenosha-protest-arsons/?sh=23a909626bfa.

143. *Id.*

threat continues growing, as law enforcement's reliance on geofence warrants dramatically increase each year.[144]

Geolocation data also reveals personal and sensitive information that can be inferred from people's whereabouts.[145] *FTC v. Kochava* exemplifies how data brokers engage in harmful commercial surveillance practices to profit from real individual's geolocation data, with the cost being user's data privacy.[146] However, the complaint's findings on tracking and identifying people at sensitive locations did not stop at reproductive health clinics.[147] Kochava's publicly-available data sample made it possible to identify and track people going to places of worship, homeless and domestic violence shelters, addiction recovery centers, and other facilities for at-risk populations.[148] This exemplifies how surveillance capitalism allows companies and their clients to target specific groups of individuals for their specific agendas. Although Google recognized the privacy threat from *Dobbs* and subsequently pledged to delete user visits to sensitive locations from their location and app history,[149] the fact that Google still tracks user's movements before and after leaving a "blackout area" effectively conceals nothing about an individual's visit to sensitive locations.[150] Location data can reveal vast amounts of personal information either on its own, or in the aggregate, which is ripe for abuse.[151]

2. *Digital and Internet Health Information*

Dobbs demonstrates that HIPAA is inadequate to protect health data stored and collected in apps and across the internet. Health information available online has dramatically increased in the past decade, with the amount of

144. *See* Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant at 3, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Dec. 23, 2019) ("Year over year, Google has observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and to date, the rate has increased over 500% from 2018 to 2019").

145. *See* Prince, *supra* note 119, at 52, 54-57.

146. *See* FTC, *supra* note 4.

147. *Id.*

148. *Id.*

149. *See* 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#:~:text=the%20main%20story-,Google%20Says%20It%20Will%20Delete%20Location%20Data%20When%20Users%20Visit,for%20the%20post%2DRoe%20era.&text=As%20a%20subscriber%2C%20you%20have,can%20read%20what%20you%20share. *See also* Jen Fitzpatrick, *Protecting people's privacy on health topics*, GOOGLE (July 1, 2022), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/.

150. *See* Edelson, *supra* note 83.

151. *See* Prince, *supra* note 119 at 52.

people turning to the internet for health questions increasing with it.[152] A survey[153] conducted from 2008 through 2017 found that the internet was the most frequently used source of health information every year, with the second source being a physician or healthcare provider.[154] However, privacy protections for health information in apps and internet searches has not kept pace with digital healthcare's utility. A person may feel that there is more privacy and less judgment in searching his or her symptoms online, but the reality is that his or her health concerns are being stored, and shared with third parties.[155] The presumed confidentiality associated with mental help does not apply to user's data, as mental help app's privacy policies leave carve outs for sharing such data with unlisted third parties.[156] A study investigating the circulation of mental health data within the databroker ecosystem found that 11 out of 37 contacted databroker firms were willing to sell mental health data, with the 10 most engaged brokers advertising highly sensitive mental health data.[157] This data included information on Americans' anxiety, bipolar disorder, ADHD, and even demographic and identifying characteristics including ethnicity, age, marital status, net worth, credit score, and more.[158] The WebMD Symptom Checker app compiles data points based on user's searches to target them with ads based on their health concerns.[159] Even hopital websites cannot escape the grasps of digitalized tracking and sharing.[160] A Markup investigation found that Meta's pixel tracking tool was

152. *See* Rutten et. al., *supra* note 101, at 617.

153. *See id*. (describing survey methodology; survey collectors used data from four administrators of Health Information National Trends Survey ("HINTS") to conduct a multivariable analysis to analyze trends over time in accessing health information, in addition to examining sociodemographic variables for those seeking health information via the internet).

154. *Id.* at 619.

155. *fSee* Tatum Hunter & Jeremy B. Merrill, *Health apps share your concerns with advertisers. HIPAA can't stop it.*, WASH. POST (Sept. 22, 2022), https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy/.

156. *Id.*

157. *See* Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data,* DUKE SANFORD CYBER POL'Y PROGRAM, 2023, at 1. https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf. (last visited Sept. 24, 2023).

158. *Id.* at 4.

159. WebMD's privacy policy states that "Even if you do not provide us with personal information, we collect non-personal information about your use of our Site." and explains how the site tracks users' "cookies" and "web beacons" to collect "anonymous" information. Despite claims that this information is anonymous, this site tracking can reveal a WebMD user's IP address, site URLs, and "the ID number of any Cookies on your computer previously placed by that server. *See Privacy Policy,* WEBMD, https://www.webmd.com/corporate/privacy (last visited Sept. 24, 2023).

160. *See* Todd Feathers & Simon Fondrie-Teitler, *Meta Faces Mounting Questions from Congress on Health Data Privacy as Hospitals Remove Facebook Tracker,* THE MARKUP (Sept. 19, 2022), https://themarkup.org/pixel-hunt/2022/09/19/meta-faces-mounting-questions-from-congress-on-health-data-privacy-as-hospitals-remove-facebook-tracker.

found on 33 of Newsweek's top 100 hospitals in the U.S.[161] These pixels collected details on patient's doctor's appointments, prescriptions, health conditions on hospital websites, and even inside their password-protected patient portals.[162]

There is no comprehensive federal law protecting all forms of digital health data.[163]

HIPAA is the primary federal law for health privacy, but most digital platforms that collect health data are not covered by HIPAA, which allows apps, social media, wearables, and other technologies to legally share, license, and sell users' health data to third parties without user's knowledge or consent.[164] With no broad federal protections, the legwork falls on state laws and tech companies to implement privacy protections. However, there are only five U.S. states with consumer privacy laws.[165] For the remaining 45 states, privacy protections essentially hinge on notice and consent provided by tech companies to users for its service, thereby shifting the burden to lay people to navigate complex privacy notices of disclosure.[166] The average person does not have the time or skillset to divulge into a company's terms and conditions. A study quantifying the time it would take to read company policies and the value of that time exerted, estimated that it would take all Americans 54 billion hours annually to read online privacy policies each time they visit a new site, which has a value of approximately $781 billion.[167] This is an unfair and infeasible burden to shift to the average internet user, especially where an individual is looking to receive help without being subject to an invasion of his or her privacy.

Dobbs has left women urgently scrambling to self-manage their reproductive health privacy, and brought that struggle to the spotlight. However, the general lack of comprehensive privacy protections for internet health data

161. *Id.*

162. *Id.*

163. *See generally,* Richard Sobel, *The HIPAA Paradox: The Privacy Rule That's Not,* 37, THE HASTINGS CTR. 40, 40-50 (2007), https://www.jstor.org/stable/pdf/4625762.pdf?casa_token=wUFcMo6iUGYAAAAA:a_2czasQxkp87DpSAxwFzKd-biEo347f9FKFE53z_lOuoSHM5cESQ4F30UuwO1Uw91NaljiRoZZ1WNKpaMpPRr5NEeI7Jd8SuHINZV1wzWtoKoE3YdOs (Discussing the gaps in HIPAA that prevent broad protections for private health information).

164. *See* Kim, *supra* note 157, at 2.

165. *See* Sherman, *supra* note 125.

166. *See e.g., In re* Facebook Consumer Privacy User Profile Litigation, Dkt. No. 18-md-02843 (N.D. Cal. June 6, 2018), ECF No. 1096. sec IV (illustrating the complexity of user consent, as well as how consent is interpreted differently based on state laws. Here, California uses a contracts interpretation of consent, while other states do not).

167. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 J. OF L. AND POL'Y FOR THE INFO. SOC'Y 3, 543 AT 563-64, (2008), http://hdl.handle.net/1811/72839.

does not exclusively apply to women. The gaps in the current federal framework coupled with largely unregulated company procedures for health data collection infringe on the vast majority of Americans' privacy who wish to utilize the internet's convenience and cost-effectiveness to treat their health issues.

IV. REMEDIES TO PRIVACY HARMS

A. A Comprehensive Federal Framework

There must be a comprehensive federal law that addresses all types of data accessed by companies. As discussed in section II, the US privacy landscape is governed by different agencies, with various laws that operate in silos and cover specific types of data in specific circumstances.[168] Without a comprehensive federal framework covering all types of data rather than a patchwork of narrow statutes, privacy harms will slip through the cracks. While implementing comprehensive legislation is by no means an easy task, the United States should strive to emulate something similar to the European Union's General Data Protections Regulation (GDPR).[169] The GDPR imposes obligations – such as fairness, transparency, accuracy, storage limitation, and accountability – on all organizations that collect data from people in the EU.[170] The GDPR has a large breadth of coverage, and imposes large fines on violators for deterrence, making it "the toughest privacy and security law in the world."[171] The GDPR is not a privacy law that takes a sectoral approach like the U.S., but rather an "omnibus data protection regime" governing the processing of personal data.[172] Simply, the GDPR provides a preventative approach by imposing requirements that protect consumers from illegitimate data collection, while the US imposes security requirements only after the data has been collected.[173] In the post-*Dobbs* landscape, this preventative approach would better shield women's personal reproductive data from collection and storage from data brokers to be provided to law enforcement. It could also provide the transparency that is currently lacking in the data broker ecosystem when collecting, for instance, mental health data by requiring a company to "demonstrate[] compelling legitimate grounds for

168. *See* Klosowski, *supra* note 53.

169. *See* Fowler & Ulrich, *supra* note 89, at 63.

170. *See What Is Gdpr, The Eu's New Data Protection Law?*, GDPR, https://gdpr.eu/what-is-gdpr/ (last visited Sept. 24, 2023).

171. *Id.*

172. *See* Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98, DENV. L. REV. 93,114 (2020).

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

the processing which override the interests, rights, and freedoms of the data subject" based on the data subject's right to object to data processing.[174]

B. State Legislation for Privacy Protection

States with abortion restriction or criminalization laws should enact consumer protection laws to soften the blow to women's autonomy post-*Dobbs*. The gaps in the current federal privacy patchwork shift the heavy-lifting to the states for privacy violation redress. As previously discussed, only five U.S. states have comprehensive consumer privacy protections, leaving the remaining 45 dependent on federal statutes or self-regulation for redress.[175] None of the five states with consumer privacy protections – California, Colorado, Connecticut, Utah, and Virginia[176] – have completely criminalized abortion.[177]

Abortion has always been a hot-button issue, with attitudes influenced by variables such as partisanship, religion, age, race, and education level.[178] However, studies support that the vast majority of Americans want greater control over their personal information and feel that the risks outweigh the benefits of data collection by companies and the government.[179] With roughly six out of every ten Americans believing it is impossible to go through daily activities without their data being collected,[180] it is likely that a person who may disfavor abortion will want greater privacy protections. Therefore, states with abortion restrictions should be able to pass digital privacy protection legislation without facing the heated partisan divide that abortion laws are subject to. By passing stronger digital privacy protections, states can protect women from the ongoing post-Dobbs privacy invasions. Ideally, states could protect women from criminalization by enacting privacy

174. *See* Jones & Kaminski, *supra* note 172, at 117 (quoting GDPR, *supra* note 160).

175. See *supra* Sec. III(B)(2).

176. *See State Laws Related to Digital Privacy,* NAT'L CONF. OF STATE LEGISLATURES, https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,comprehensive%20consumer%20data%20privacy%20laws (last updated June 7, 2022).

177. *See Tracking the States Where Abortion is Now Banned, supra* note 12.

178. *See* Allison Durkee, *How Americans Really Feel About Abortion: The Sometimes Surprising Poll Results As Supreme Court Overturns Roe v. Wade*, FORBES (June 24, 2022), https://www.forbes.com/sites/alisondurkee/2022/06/24/how-americans-really-feel-about-abortion-the-sometimes-surprising-poll-results-as-supreme-court-reportedly-set-to-overturn-roe-v-wade/?sh=2fadc7de2f3a (noting however, that there is overall broad support for abortion rights at 81% in May 2021).

179. *See* Brooke Auxier & Lee Rainie, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over their Personal Information,* PEW RSRCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

180. *Id.*

laws that are not subject to exceptions for law enforcement, like the carve-outs in the current federal laws and legislative proposals.[181]

C. Private Sector Responsibility

While courts have not recognized data privacy harm for risk of future injury, the wake of *Dobbs* prevents tech companies from claiming ignorance or misunderstanding exactly who might misuse personal data and for what purposes.[182] Tech companies are now trying to rebrand themselves as proponents of privacy,[183] with Google promising to delete location data from visits to sensitive areas or Flo offering an anonymous profile option.[184]

There are multiple protections that Big Tech can implement to protect consumers. The Electronic Frontier Foundation (EFF) provides suggestions for companies to protect users' digital privacy in light of *Dobbs,* including an opt-in for behavioral tracking, encrypting data in transit, not installing location data broker softwareinto their apps, and vetting third parties that data collected from their apps are shared with.[185] Femtech app developers can also employ preventative privacy protections by limiting data collecting to only that which is specifically necessary to menstruation or fertility predictions.[186] Less data collected means less information shared with third parties for potentially nefarious purposes.[187] Companies should protect their users' data by challenging improper demands from law enforcement, such as geofence warrants and unlawful subpoenas.[188] Big Tech can also fill the gaps in the current federal framework through independent, privatesector regulatory programs.[189] Private sector regulation for data use and collection remains voluntary.[190] However, companies can distinguish themselves from competitors by establishing rules and procedures, codes of conduct, and even avenues for consumer complaints to facilitate corrective action.[191]

181. *See* Fowler & Ulrich, *supra* note 89, at 1297.

182. *See* Edelson, *supra* note 83.

183. *See id.*

184. *See* Travis, *supra* note 84.

185. *See* Corynne McSherry & Katherine 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.

186. *See* Fowler & Ulrich, *supra* note 89, at 1304.

187. *See id.*

188. *See* McSherry & Trendacosta, *supra* note 185.

189. *See* Fowler & Ulrich, *supra* note 89, at 1303.

190. *Id.* at 1304.

191. *Id.*

CONCLUSION

The *Dobbs* decision has upended women's bodily autonomy, and further subjects her digital privacy to subsequent invasions by law enforcement and data brokers alike. *Dobbs* illustrates in real time the perniciousness of unbridled surveillance capitalism in the digital era. The primary effect of the Supreme Court's decision directly jeopardizes women's privacy in her health and location data, her search history, and enables commodification of this information through the data broker ecosystem. However, Dobbs also illuminates the fact that not only is women's data subject to these invasive practices; rather, all of our data is subject to this level of surveillance. State laws criminalizing exercise of bodily autonomy is the only wall separating the general population from the anxiety that women who do not want motherhood forced upon her are currently facing post-Dobbs with regard to data privacy. Dobbs has implications for the security of sensitive health data beyond women. Mental health data has been bartered and traded by data brokers for profit. Geofences have been utilized to interfere with exercising a constitutional right. A person's data is a reflection of their person. Their searches reflect their needs; their location tracking provides a map of their life, all which can be aggregated into a dossier by data brokers. Under the current data landscape, virtually nothing prevents that from being categorized, advertised, and sold to data brokers for reasons beyond one's knowledge or consent. Ending this invasiveness would take action at the federal, state, and private sector levels. The federal landscape must provide a comprehensive framework that covers all forms of data as opposed to the current patchwork that provides narrow protections for specific types of data. States have an interest in enacting legislation that protects consumer privacy to fill the gaps in the current federal patchwork. The private sector should take greater accountability for their role in what has happened to women post-Dobbs. Because they can no longer claim ignorance, companies should protect its consumers by collecting less data, and providing greater transparency.

***