Washington Law Review Online

Volume 98 Article 1

2024

A Loophole in the Fourth Amendment: The Government's Unregulated Purchase of Intimate Health Data

Rhea Bhatia
University of Washington School of Law

A LOOPHOLE IN THE FOURTH AMENDMENT: THE GOVERNMENT'S UNREGULATED PURCHASE OF INTIMATE HEALTH DATA

Rhea Bhatia*

Abstract: Companies use everyday applications and personal devices to collect deeply personal information about a user's body and health. While this "intimate health data" includes seemingly innocuous information about fitness activities and basic vitals, it also includes extremely private information about the user's health, such as chronic conditions and reproductive health. However, consumers have no established rights over the intimate health data shared on their devices. Believing that these technologies are created for their benefit, consumers hand over the most intimate aspects of their lives through health-related applications relying on the promise that their data will remain private. Today, the intimate health data of unaware consumers is collected and sold to third-party data brokers who then repackage the data, label it, and sell it to the highest bidder: advertisers, corporations, and most concerning of all—the government and law enforcement agencies. This ability for governmental entities to simply purchase intimate health data from third-party data brokers violates the Fourth Amendment of the United States Constitution.

To discourage the overreach of arbitrary law enforcement, the Fourth Amendment protects individuals from unreasonable searches and seizures. Without a warrant, governmental entities may purchase intimate health data from third-party data brokers, constituting an unreasonable search in violation of the Fourth Amendment. This Comment examines the use of third-party data brokers by government agencies to collect and analyze intimate health data. In doing so, this Comment advocates for greater accountability in government data collection practices and proposes legislative solutions to regulating the government's purchase of intimate health data.

INTRODUCTION

In 2019, journalist Kashmir Hill requested a consumer report from Sift, a company that tracks 16,000 types of consumer factors through its proprietary scoring system for companies such as Airbnb and OkCupid.[1] These factors encompass online service interactions such as app usage on cell phones, IP addresses, Airbnb user messages, and Yelp orders.[2] Sift

*J.D. Candidate, University of Washington School of Law, Class of 2024. Thank you to my advisor, Professor Ryan Calo, for his guidance and expertise. My sincere gratitude to Professor Inyoung Cheong for her thoughtful insights and encouragement. Special thanks to the editors of *Washington Law Review*—Ryan Lin, Danielle Igbokwe, Brian Honaker-Coe, and particularly Aldrin Jude Panganiban—for their exceptional editing acumen. Finally, thank you to my loving family, friends, and my partner Abhi, for their unwavering support.

1. Kashmir Hill, *I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too*, N.Y. TIMES (Nov. 4, 2019), https://www.nytimes.com/2019/11/04/business/secret-consumer-score-access.html [https://perma.cc/D85C-38LN].

2. *Id.*

uses these factors to "score" consumers and judge whether or not a consumer can be "trusted."[3] Companies value the collection of this data as it helps them identify and prevent fraud while increasing revenue from high-spending customers.[4] Hill paid a fee and ordered her file, receiving over 400 pages that contained messages sent to Airbnb hosts, Yelp delivery orders, and a time log demonstrating when she opened the Coinbase app on her iPhone.[5] Hill was shocked that corporations had such granular data about her life. While the collection of this type of data may seem harmless, "obscure companies . . . accumulating information about years of our online and offline behavior is unsettling, and at a minimum, it creates the potential for abuse or discrimination."[6] The fact that countless other companies other than Sift actively amass staggering amounts of information about the intimate aspects of consumers' lives makes this problem particularly disconcerting.[7]

Businesses collect data to enhance consumer experiences and develop more effective marketing strategies. Many businesses operate with personal data as a fungible commodity: one they can collect, buy, and sell. The collection and analysis of consumer data has become an integral part of modern commerce.[8] Accordingly, this collection of data allows companies to infiltrate every intimate aspect of consumers' lives, enabling them to collect and store individual "profiles" of each consumer.[9]

When it comes to health data, individuals have different levels of control over their own information depending on factors such as the type of data collected, the source of the data, and the context in which they use the data. For instance, an individual may have a high degree of bodily agency when they make the decision to improve their health by tracking their health data using a fitness app or wearable device. However, if third parties share this data without consumer consent, it compromises their bodily agency. Through fitness trackers and health apps, users have become accustomed to monitoring their own health. Although these apps are marketed as a benefit for consumers to track their health, companies collecting this health data are the real beneficiaries.

---

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.*

8. *See* Thorin Klosowski, *Big Companies Harvest Our Data. This Is Who They Think I Am*, N.Y. TIMES (May 28, 2020), https://www.nytimes.com/wirecutter/blog/data-harvesting-by-companies/ [https://perma.cc/MS2D-KTX9].

9. *Id.*

Companies profit off of health data by amassing vast troves of information on individuals and selling it to businesses, organizations, and most notably, the government.[10] This raises serious concerns regarding consumer privacy and warrantless government surveillance of intimate health data related to our bodies.[11] Despite the protections afforded to an individual's body by the Fourth Amendment, personal information associated with an individual's body lacks protection.

The Fourth Amendment protects individuals from unreasonable searches and seizures by requiring government agencies, prior to conducting a search, to obtain a warrant based on probable cause.[12] While exceptions to the warrant requirement exist, the government's purchase of intimate data from third-party data brokers does not typically fall within these exceptions.[13] Because the ability for governmental entities to simply purchase intimate health data from third-party data brokers circumvents the warrant requirement under the Fourth Amendment, protecting consumers from government purchases of health data lacks a proper legal mechanism.

The Health Insurance Portability and Accountability Act (HIPAA) does not cover intimate health data purchased by the government.[14] Health data collected from applications and devices contain intimate information about a person's physical, mental, and emotional well-being, which make up the most private information about their bodies. By examining these data points in conjunction with one another, the government can gain a more holistic view of how an individual's decisions relate to their body. This type of unauthorized utilization of personal health information beyond its original purpose poses a significant threat to an individual's autonomy and control over their own body and health. Consumers should have protections to maintain agency over these data points, especially when influential entities like the government possess them. Therefore, the acquisition of health data by the government from third-party data brokers is a concerning loophole within the framework of the Fourth Amendment.

---

10. *See* Wolfie Christl, *Corporate Surveillance in Everyday Life*, CRACKED LABS (June 2017), https://crackedlabs.org/en/corporate-surveillance [https://perma.cc/P7FN-MEDG].

11. *See* Sean Lyngaas, *US Intelligence Agencies Buy Americans' Personal Data, New Report Says*, CNN (June 12, 2023), https://www.cnn.com/2023/06/12/politics/intel-agencies-personal-data/index.html#:~:text=The%20vast%20amount%20of%20personal,newly%20declassified%20US%20intelligence%20report [https://perma.cc/592R-ETDL].

12. U.S. CONST., amend. IV.

13. *See Exigent Circumstances*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/exigent_circumstances [https://perma.cc/5SVU-Q9UU] (last updated Dec. 2022).

14. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

This Comment proceeds in four parts. Part I explains the foundation of the Fourth Amendment. It then provides an overview of the limited application of the third-party doctrine, how third-party data brokers collect data, and how data brokers interact with governmental agencies. Part II examines the scope of intimate health data and how the government collection of this type of data puts certain groups at risk, such as those seeking abortions. Part III outlines both the existing and proposed legislation that attempts to regulate the government's collection of intimate data. Finally, Part IV provides recommendations to amend the proposed legislation to advocate for greater protection of intimate health data.

I. FOURTH AMENDMENT AND THIRD-PARTY DATA BROKERS

This Part explores the intersection of the Fourth Amendment, the third-party doctrine, and the role of third-party data brokers in government surveillance. First, section I.A examines both the limitations of Fourth Amendment protections when third parties collect personal data, and the Stored Communications Act's[15] attempt to address concerns regarding government access to electronic communication. Second, section I.B introduces third-party data brokers, their methods of data collection, and the extensive consumer profiles they create. Finally, section I.C explains how third-party data brokers assist government agencies in bypassing Fourth Amendment protections.

A. Fourth Amendment and the Third-Party Doctrine

The Fourth Amendment of the U.S. Constitution safeguards against unlawful searches and seizures[16] and typically requires law enforcement officials to obtain a warrant before collecting personal data.[17] However, the Fourth Amendment's protections seldom apply when an official is collecting information about an individual from a third party.[18] For example, the United States Supreme Court has held that Fourth Amendment protections do not apply when law enforcement seeks a

15. 18 U.S.C. §§ 2701–12 (2021).

16. U.S. CONST., amend. IV.

17. *See* CHRIS D. LINEBAUGH, CONG. RSCH. SERVS., ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW (2d ed. 2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10786 [https://perma.cc/7359-CW6A].

18. *Id.*

suspect's financial records maintained by a bank[19] or phone records displaying the dialed phone numbers of the suspect.[20] The Court's rationale behind this is the third-party doctrine.[21] This doctrine asserts that when individuals share their information with a third party, such as a bank or a telephone provider, they no longer maintain a reasonable expectation of privacy in that information.[22] Thus, the government can access that information without first acquiring a warrant.[23]

To address growing privacy concerns under the third-party doctrine, Congress passed the Stored Communications Act (SCA).[24] The SCA was passed as Title II of the Electronic Communications Privacy Act of 1986 (ECPA),[25] to expand and revise federal wiretapping and electronic eavesdropping provisions.[26] The SCA provides statutory privacy protections for stored electronic communications in cases where these communications might not be covered by the Fourth Amendment under the third-party doctrine.[27] It was enacted to promote "the privacy expectations of citizens and the legitimate needs of law enforcement."[28] The SCA prohibits providers from disclosing electronic communications to any individual or entity, except in a few exceptions, such as when the government requires such information.[29] Although the SCA restricts certain entities from voluntarily sharing consumer data with the government, it does not prevent providers from sharing customer data with private entities. Consequently, there are no restrictions preventing

---

19. *See e.g.,* United States v. Miller, 425 U.S. 435 (1976) (holding that the disclosure of a customer's bank records did not constitute a Fourth Amendment search because the defendant had no reasonable expectation of privacy by voluntarily conveying information to the banks in the ordinary course of business).

20. *See e.g.,* Smith v. Maryland, 442 U.S. 735 (1979) (holding that the installation and use of a pen register to record dialed numbers from a petitioner's telephone did not constitute a Fourth Amendment search because the petitioner had no reasonable expectation of privacy by voluntarily conveying numerical information disclosed to the telephone company in the ordinary course of business).

21. *See generally Miller*, 425 U.S. at 435; *see generally Smith*, 442 U.S. at 735. Both decisions paved the way for the creation of the third-party doctrine.

22. LINEBAUGH, *supra* note 17, at 2.

23. *See Miller*, 425 U.S. at 435; *see also id.*

24. 18 U.S.C. §§ 2701–12 (2021).

25. Electric Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–22.

26. *See Electric Communications Privacy Act (ECPA),* ELEC. PRIV. INFO. CTR., https://epic.org/ecpa/ [https://perma.cc/V6R5-Q8WB].

27. *See* JIMMY BALSER, CONG. RSCH. SERV, OVERVIEW OF GOVERNMENTAL ACTION UNDER THE STORED COMMUNICATIONS ACT (SCA) 2 (1st ed. 2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10801 [https://perma.cc/UK29-4VPN].

28. *Electric Communications Privacy Act (ECPA), supra* note 26 (quoting H.R. REP. NO. 99-647, at 19 (1986).

29. BALSER, *supra* note 27, at 2.

third-party data brokers from subsequently sharing this customer data with the government.[30]

However, the Supreme Court recognized a limit to the third-party doctrine in *Carpenter v. United States*.[31] In *Carpenter*, law enforcement arrested Timothy Carpenter in connection with a series of T-Mobile store robberies.[32] An accomplice confessed to the crime and provided Carpenter's cell phone number to the police.[33] By using Carpenter's cell phone number, law enforcement then accessed Carpenter's cell-site location information (CSLI) records pursuant to section 2703(d) of the SCA, allowing law enforcement to make requests with a low evidentiary threshold.[34] Because the CSLI revealed the suspect's detailed movements over the course of 127 days, the Court declined to apply the third-party doctrine and held that law enforcement's collection of customers' historical CSLI from cell phone providers violated the Fourth Amendment.[35] While the CSLI data Carpenter shared with his wireless carrier were considered business records, the Court reasoned that they were nonetheless "unique" and of a "qualitatively different category" of business records than what the third-party doctrine typically excludes from Fourth Amendment protection.[36]

However, *Carpenter* was a narrow decision, finding that only the government's acquisition of seven days or more of historical CSLI from a wireless carrier constituted a search under the Fourth Amendment.[37] Due to this narrow interpretation, no legal mechanism actively hinders the government from purchasing data from third-party data brokers.[38] *Carpenter* does not regulate the practices of data brokers because the Fourth Amendment does not regulate open market transactions.[39] The government no longer needs to compel data production from providers because various apps and devices collect vast amounts of personal data that can be packaged and sold to the government without a warrant.[40]

---

30. Dori H. Rahbar, *Laundering Data: How the Government's Purchase of Commercial Location Data Violates Carpenter and Evades The Fourth Amendment*, 122 COLUM. L. REV. 713, 724 (2022).

31. Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206 (2018).

32. *Id.* at 2212.

33. *Id.*

34. *Id.*

35. *Id.* at 2209.

36. *Id.* at 2209–16.

37. *Id.* at 2220.

38. *See* Rahbar, *supra* note 30, at 724.

39. *Id.*

40. *See* Elizabeth Goitein, *The Government Can't Seize Your Digital Data. Except by Buying It*, WASH. POST (Apr. 26, 2021), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/ [https://perma.cc/R5MW-L953].

When this data is aggregated, it can reveal intimate information that customers never consented to share with the government. Thus, many companies sell information to third-party data brokers who then sell it to the government.[41]

B. Third-Party Data Brokers

Third-party data brokers are companies that collect and then sell the personal information of customers to other companies. They essentially function as the middlemen of surveillance capitalism: collecting information from consumers, consolidating it, and selling it.[42] Data brokers "own and store billions of data points pertaining to anyone who inhabits the digital space, and then use these points to generate inferential data, placing the brokers among the most powerful organisations in today's digital world."[43] In 2004, approximately 500 companies were peddling out personal data.[44] In 2020, an estimated 5,000 data brokers now work worldwide.[45] Data brokers collect information in numerous ways, including buying it from third-party companies (such as credit card companies or free applications), searching public databases (such as court records, housing records, or social media), and directly tracking user activities online.[46] For example, brokers can use cookies, which are small

41. *See* Katherine Hamilton, *U.S. Government Buying 'Intimate' Data About Americans, Report Finds*, FORBES (June 12, 2023), https://www.forbes.com/sites/katherinehamilton/2023/06/12/us-government-buying-intimate-data-about-americans-report-finds/?sh=6404f260645d [https://perma.cc/6TFF-NYZS].

42. *See generally* Justin Sherman, *Data Brokers Are a Threat to Democracy*, WIRED (Apr. 13, 2021), https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/ [https://perma.cc/25PQ-748K].

43. Henrik Twetman & Gundars Bergmanis-Korats, *Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data*, NATO STRATEGIC COMM. CTRE. OF EXCELLENCE 6–7 (Jan. 20, 2020), https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf [https://perma.cc/47DB-B4FF].

44. DANIELLE CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE 5 (2022).

45. Twetman & Bergmanis-Korats, *supra* note 43 at 9. "Some of the top players in this market are Acxiom, Experian, Equifax, CoreLogic, TransUnion, Oracle, Lifelock, H.I.G. Capital, PeekYou, and TowerData." *Id.*

46. Acxiom runs one of the world's largest commercial databases on consumers. Shimon Brathwaite, *What Does a Data Broker Do*, SEC. MADE SIMPLE (Feb. 2, 2021), https://www.securitymadesimple.org/cybersecurity-blog/what-does-a-data-broker-do [https://perma.cc/GT6Y-YWA8]. The company provides up to 3,000 data elements on people from thousands of sources in many countries, including the United States, the United Kingdom, and Germany. *Id.* Acxiom sells access to its extensive consumer profiles and helps clients find, target, identify, analyze, sort, rate, and rank certain individuals. *Id.* The company also directly manages 15,000 customer databases with billions of consumer profiles for its clients, including large banks, insurers, healthcare organizations, and government agencies. *Id.*

packets of data that help websites function, to log the online activity of consumers.[47] Additionally, brokers may use browser fingerprinting, aided by invisible scripts, to track users across websites and identify consumers via browser, device, language, and time zone.[48]

Upon signing up for a site or application, users often tick a box that states something to the effect of "you agree we can share your data with select third-party partners."[49] By ticking the box, the data may be sold to third-party data brokers. Similarly, many free apps—including major social media companies and delivery apps—sell the data they collect to third parties.[50] In a recent study, the Federal Trade Commission (FTC) studied twelve different health and fitness apps and found they sent data to seventy-six different third parties.[51] This data encompassed consumer device identifiers and details, personalized identifiers, along with consumer health data like exercise habits, dietary patterns, and symptom searches.[52] This is not the first report to demonstrate this, and a quick review of any health app's privacy policy illustrates that many apps collect data for use in advertising.[53]

After collecting consumer information, "data brokers aggregate that information into segments or marketable categories, often through automated predictive analysis tools."[54] Third-party data brokers use predictive algorithmic assessments to rate users.[55] Data brokers rank individuals based on their likelihood to vote or assess job candidates according to their creativity and leadership skills.[56] They take strings of

---

47. *See generally* Nica Latto, *Data Brokers: Everything You Need to Know*, AVAST ACAD. (Oct. 29, 2020), https://www.avast.com/c-data-brokers [https://perma.cc/JQ4F-4DBT].

48. *Id.*

49. Harry Guinness, *How Data Brokers Threaten Your Privacy*, POPULAR SCI. (May 25, 2022), https://www.popsci.com/technology/data-brokers-explained/ [https://perma.cc/UA4S-59TJ].

50. Brathwaite, *supra* note 46.

51. Jared Ho, Presenter for the Federal Trade Commission Spring Privacy Series on Consumer Generated and Controlled Health Data 28 (May 7, 2014), https://www.ftc.gov/system/files/documents/public_events/195411/2014_05_07_consumer-generated-controlled-health-data-final-transcript.pdf [https://perma.cc/N28N-B4NC].

52. *Id.*

53. *See* Greg Slabodkin. *FTC Concerned with Health Data Sharing Apps*, HEALTH DATA MGMT. (May 8, 2014), https://www.healthdatamanagement.com/articles/ftc-concerned-with-health-data-sharing-apps [https://perma.cc/Y2F9-EDUZ].

54. Lauren Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security*, 60 B.C. L. REV. 349, 351 (2019).

55. *See* CITRON, *supra* note 44, at 12.

56. *Id.*

data and turn users into "ranked and rated objects."[57] Examples of these marketable categories include: "Winter Activity Enthusiast," "Dog Owner," or "Expectant Parent."[58]

Additionally, the profiles that data brokers have on individuals include, but are not limited to, information about education, occupation, children, religion, ethnicity, political views, activities, interests and media usage, and online behavior such as web searches.[59] Data brokers also generate predictive scores that anticipate an individual's future behavior, such as someone's economic stability, plans to have a baby, or plans to change jobs.[60]

In another study, the FTC identified several of these categories to be potentially discriminatory and harmful to consumers.[61] For example, the FTC uncovered categories that focused on the race and income levels of consumers such as "Urban Scramble" and "Mobile Mixers," which targeted low-income Latinos and African Americans.[62] In a 2013 Senate staff report on the data broker industry, third-party data brokers proffered additional targeting titles like "Rural and Barely Making It" and "Ethnic Second-City Strugglers."[63] A number of other brokers advertised their ability to categorize increasingly specific subgroups of people based on attributes such as race, gender, marital status, and income.[64] Most users would not believe these sensitive characteristics would end up on a database—let alone up for sale.[65] While it is unnerving to leave discriminatory data in the hands of companies, this issue is further heightened when intimate data is accessible to the government.

---

57. Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 3 (2014).

58. *Data Brokers: You Are Being Packaged and Sold*, SEC. THROUGH EDUC. (June 7, 2018), https://www.social-engineer.org/general-blog/data-brokers-you-are-being-packaged-and-sold/ [https://perma.cc/D99L-UYWA].

59. Christl, *supra* note 10.

60. *Id.*

61. *See e.g., FTC Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N 23–35 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/7W59-QGWQ] (finding that one data broker collected information on "1.4 billion consumer transactions and over 700 billion aggregated data elements" and another broker collected "3000 data segments for nearly every U.S. consumer").

62. *Id.*

63. STAFF OF S. COMM. ON COMMERCE, SCIENCE, AND TRANSPORTATION, A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES, 113TH CONG., REP. II (2013) https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a [https://perma.cc/CWP5-TJLY].

64. *See generally id.* at 13.

65. *Id* at 5–6.

C. Interactions Between Third-Party Data Brokers and the Government

By providing the government with intimate data without a warrant, third-party data brokers assist the government in bypassing Fourth Amendment safeguards for consumers. Federal law enforcement agencies such as the Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement (ICE), and the Internal Revenue Service (IRS) have purchased data from data brokers for use in a variety of areas, such as criminal investigations and deportations.[66] A report from the Senior Advisory Group of the Office of the Director of National Intelligence found that many governmental agencies, including the FBI and the United States Department of Defense (DOD), have contracts with data brokers to purchase "commercially available information" (CAI).[67] Although intelligence agencies have collected vast amounts of CAI, the report highlights the lack of standards and procedures governing the acquisition and use of this information.[68] The report makes it clear that agencies do not have procedures or ex ante safeguards to filter or track the vast amounts of data they are collecting—including intimate health data.[69]

Most entities acquire this data without a warrant, public disclosure, or strong oversight of the data and its uses.[70] For example, a known data broker, Thomson Reuters, supplies data brokering services to intelligence agencies and federal and local law enforcement agencies, such as the DOD and the United States Department of Justice (DOJ).[71] Additionally, entities not focused on surveillance, such as the United States Postal Service and the IRS, have begun collaborating with data companies to "'assess threats' and track fraud."[72] However, these processes operate

66. Sherman, *supra* note 42.

67. Chris Baumohl, *ODNI Report on Intelligence Agencies' Data Purchases Underscores Urgency of Reform*, EPIC (July 7, 2023), https://epic.org/odni-report-on-intelligence-agencies-data-purchases-underscores-urgency-of-reform/ [https://perma.cc/C99T-5XW4].

68. *Id.*

69. REPORT TO THE DIRECTOR OF NATIONAL INTELLIGENCE, OFF. OF THE DIR. OF NAT'L INTEL. SENIOR ADVISORY GRP. PANEL ON COM. AVAILABLE INFO. 21 (2022), https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf [https://perma.cc/8R7N-3ZSE].

70. Sherman, *supra* note 42.

71. *See generally Digital Dragnets: Examining the Government's Access to Your Personal Data: Hearing Before the H. Comm. on the Judiciary,* 117th Cong. 7 (2022) (statements of Sarah Lamdan, Professor of Law at the City University of New York School of Law) https://docs.house.gov/meetings/JU/JU00/20220719/115009/HHRG-117-JU00-Wstate-LamdanS-20220719.pdf [https://perma.cc/T8VZ-YUR4].

72. *Id.* (citation omitted).

secretly, such that no regulation exists for the type of information collected to "assess threats."[73]

Data brokers create strings of intimate health data, which are organized data points under specific categories that are easier to analyze. As these data brokers interact with numerous governmental agencies, these agencies may gain access to *packaged* intimate health data. Third-party data brokers serve as "Big Brother's Little Helpers"[74] with no legal process governing the transfer of intimate data from companies to governments. Data brokers as "little helpers" have a standing drop-off point called fusion centers to provide the government with data.[75]

Operating in major urban areas, fusion centers are state-owned-and-operated facilities that function as hubs for receiving, analyzing, gathering, and sharing threat-related information among State, Local, Tribal and Territorial entities, as well as federal agencies and private sector partners.[76] Over seventy fusion centers operate in the United States.[77] Between 2015 and 2017, state legislatures funded five fusion center positions for a total of $1.3 million.[78] With analytics software supplied by companies, fusion centers search for patterns in data broker dossiers and public and private databases.[79]

One type of fusion center, the intelligence fusion center, grew in popularity among state and local law enforcement as officers sought to enhance their intelligence capabilities to defend homeland security.[80] Fusion centers began as an outlet for agencies to pool their resources, expertise, and information to strengthen their "ability to detect, prevent,

---

73. *Id*.

74. *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. 595 (2004).

75. *Fusion Centers*, U.S DEP'T OF HOMELAND SEC., https://www.dhs.gov/fusion-centers [https://perma.cc/J7L4-NBZ3] (last updated Oct. 17, 2022); *see e.g.,* Hoofnagle, supra note 74, at 595 (finding that data brokers collect information tailored to law enforcement for distribution to fusion centers, acting as "little helpers").

76. *Fusion Centers*, supra note 75.

77. Amanda Peacher, *Why Is the State of Oregon Conducting Intelligence Work?*, OPB (Apr. 26, 2016), https://www.opb.org/news/article/oregon-department-of-justice-intelligence/#:~:text=Analysts%20research%20potential%20threats%20in,for%20event%20preparation%20and%20security [https://perma.cc/C4L6-CZLZ].

78. Some centers are funded via grants or federal money, according to the DOJ. *Id.*

79. CITRON, *supra* note 44, at 58.

80. Michael German & Jay Stanley, *What's Wrong with Fusion Centers?*, ACLU 6 (Dec. 12, 2007), https://www.aclu.org/sites/default/files/pdfs/privacy/fusioncenter_20071212.pdf [https://perma.cc/N8DT-WGNS].

investigate, and respond to criminal and terrorist activity."[81] Beginning in 2003, these centers evolved independently to cater to local and regional needs.[82] Fusion centers broadened their sources of data "beyond criminal intelligence, to include federal intelligence as well as public and private sector data."[83] This growth took place in the absence of any legal framework for regulating fusion center activities. This lack of regulation quickly led to "'mission creep,' in which fusion centers originally justified as anti-terrorism initiatives rapidly drifted toward an 'all crimes, all-hazards' policy that is 'flexible enough for use in all emergencies.'"[84]

According to the United States Department of Homeland Security, the fusion center mantra is "the more data, the better."[85] Data brokers provide fusion centers with access to any kind of data. In 2021, a group of social justice advocates filed a lawsuit against the Oregon Department of Justice for its illegal surveillance operation, known as the Oregon Terrorism Information Threat Assessment Network (TITAN) fusion center.[86] In 2015, the Oregon TITAN fusion center used a surveillance tool called "Digital Stakeout" to monitor tweets of Salem residents who expressed opposition to police violence against African Americans.[87] In 2019, this fusion center was also caught creating intelligence reports on environmental protestors who objected to fossil fuel infrastructure projects in the state.[88] In response, forty-five leaders from international,

---

81. *Id*. at 7 (quoting BUREAU OF JUSTICE ASSISTANCE, OFFICE OF JUSTICE PROGRAMS, U.S. DEP'T OF JUSTICE, FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION AND INTELLIGENCE IN A NEW ERA 2 (2006) https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_guidelines_law_enforcement.pdf [https://perma.cc/DK6C-W5F6].

82. *Id.* at 6.

83. *Id.* at 7 (quoting TODD MASSE, SIOBHAN O'NEIL & JOHN ROLLINS, CONG. RSCH. SERV, FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS 1 (2007) https://www.everycrsreport.com/files/20070706_RL34070_5fd3cb9c25ff80d8e4517d9b4b21323c88fb61ca.pdf [https://perma.cc/A5SR-DBH4].

84. *Id.* at 6. (quoting TODD MASSE, SIOBHAN O'NEIL & JOHN ROLLINS, CONG. RSCH. SERV, FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS 22 (2007) https://www.everycrsreport.com/files/20070706_RL34070_5fd3cb9c25ff80d8e4517d9b4b21323c88fb61ca.pdf [https://perma.cc/A5SR-DBH4].

85. CITRON, *supra* note 44, at 58 (quoting Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L. J. 1441, 144855 (2011)).

86. *Oregan Sued Over Domestic Spying Operation*, POLICING PROJECT (Dec. 14, 2021), https://www.policingproject.org/news-main/2021/12/21/oregon-sued-over-domestic-spying-operation [https://perma.cc/L7KQ-HW2M].

87. Investigation Report at 7, Johnson v. Rosenblum et. al, No. 6:16-cv-02052 (D. Or. Apr. 6, 2016), http://media.oregonlive.com/politics_impact/other/investigation.pdf [https://perma.cc/FM6V-M5MM].

88. Will Parrish & Jason Wilson, *Revealed: Anti-error Center Helped Police Track Environmental Activists*, THE GUARDIAN (Oct. 2, 2019), https://www.theguardian.com/us-news/2019/oct/02/oregon-pipelines-protests-monitoring-police-anti-terror-unit [https://perma.cc/ZK45-3LNH].

national, and Oregon-based organizations wrote a letter to Oregon Governor Kate Brown, urging her to cease the state's cooperation with any surveillance of activists.[89] Environmentalists also responded, such as prominent activist Bill McKibben, who argued that "monitoring and compiling information about Oregonians' political or social views, activities, or associations violate[d] Oregon law," and asked that the governor protect the civil liberties of Oregon residents by withdrawing from the task force that utilizes the fusion center.[90] These instances underscore the government's capacity to utilize data supplied to fusion centers for purposes unrelated to countering terrorist threats, shedding light on its extensive access to individual data. Like the data collected on environmental protestors without their consent, the limited regulation surrounding the collection of intimate health data by third-party brokers merits a high level of protection.

II. SCOPE AND RISKS OF INTIMATE HEALTH DATA COLLECTION

Part II of this Comment will examine the scope of intimate health data and the risks of unregulated data collection. Section II.A will explain how certain types of health information are collected and used. Section II.B will examine the lack of protection under HIPAA for intimate health data collected by third-party data brokers. Section II.C illustrates the risks imposed on different groups of people once third-party data brokers categorize and sell their health data. Finally, section II.D will address the amplified risks associated with the unregulated collection of reproductive health data.

A. Scope of Intimate Health Data

The definition of intimate data could vary from context to context. For the purpose of this Comment, intimate data is defined as the data that represents information related to an individual's body, health status, and health-related choices. This includes not only general health apps, but also data collected from fitness trackers and reproductive and sexual health apps. This Comment focuses particularly on health-related data that operate as personal unique identifiers for consumers.

Among the most common devices that collect consumer health data are fitness bands. Consumers use fitness bands such as the Amazon Halo (Halo) or Apple Watch to track sleep cycles, tone of voice, body fat

89. *Id.*

90. *Id.* (citation omitted).

percentage, blood oxygen levels, heart rate, and level of fitness activity.[91] In particular, the Halo initially gathered an unprecedented level of intimate personal data before being discontinued.[92] The Halo collected intrusive forms of personal information, such as body photos and voice recordings, which were then inputted into Amazon's software for analysis.[93]

Two of the features that the Halo offered were a body fat percentage feature and a tone feature.[94] With the body fat percentage feature, users were asked to wear minimal clothing and take pictures of their bodies from four different angles to allow the app to calculate their body fat percentage.[95] The app also recommended repeating the process of sending photos every two weeks to track progress.[96] As for the tone feature, the Halo asked the user to read sample phrases in order to recognize their voice, and then also tracked moments in the user's conversations throughout the day that go beyond their neutral tone.[97] By plotting these moments as positive versus negative and high versus low energy, the Halo applied nuanced descriptors to them.[98] For instance, a voice registering as negative and low energy might be categorized as "discouraged."[99] On its face, the Halo provided users with an efficient way to track their health progress and meet their fitness goals. However, Amazon has not pledged to properly handle these photos and intimate data to help users.

Before the Halo was discontinued, Amazon was planning to launch a health coaching service where an artificial intelligence (AI) trainer would use webcam and movement scanning to assess a user's workouts and monitor their progress.[100] The AI trainer would add form tracking, rep counting, and detailed performance metrics in a post-workout

---

91. Geoffrey A. Fowler & Heather Kelly, *Amazon's New Health Band Is the Most Invasive Tech We've Ever Tested*, WASH. POST (Dec. 10, 2020),https://www.washingtonpost.com/technology/2020/12/10/amazon-halo-band-review/ [https://perma.cc/S866-BQAX].

92. *Id.; see also* Chris Welch, *Inside Amazon's Canceled Plan to Make Halo a Fitness Success*, THE VERGE (May 1, 2023), https://www.theverge.com/2023/5/1/23704825/amazon-halo-canceled-features-ai-training-apple-watch [https://perma.cc/87PD-TZT8].

93. Fowler & Kelly, *supra* note 91.

94. *Id*.

95. *See* Sophie Webster, *Amazon's Halo Body Fat Percentage Scanner Is a Benchmark for Those Looking for Information About Their Bodies*, TECH TIMES (June 17, 2021), https://www.techtimes.com/articles/261610/20210617/amazons-halo-body-fat-percentage-scanner-benchmark-those-looking-information.htm [https://perma.cc/LF8M-2JDK].

96. *Id.*

97. Fowler & Kelly, *supra* note 91.

98. *Id.*

99. *Id.*

100. Welch, *supra* note 92.

summary.[101] An article reviewing the Halo stated that "[t]he amount of data Amazon collected on [Halo] customers is incredible."[102] However, the feedback from the initial AI trainer's performance was not positive, and Amazon's own staff raised concerns about a camera recording individuals during their workouts and then sharing the data with Amazon.[103] This intimate data could have ultimately been collected in a completely unregulated ecosystem.

Our society has become accustomed to an increased amount of surveillance due to the expansion and increased reliance on technology, especially when it comes to health data. Many users rely on smartphone apps to increase convenience in their day-to-day lives without even batting an eye. For example, a 2019 survey from the Kaiser Family Foundation found that nearly one-third of women in the United States use some type of period tracking app.[104] According to Frost & Sullivan, a research and consulting firm, the market for all digital tools for women's health needs could be worth as much as fifty billion dollars by 2025, and this includes apps for personalized nutrition advice, period tracking, weight loss, and high-tech breast pumps that record when and how much breast milk is pumped.[105] One startup named Flo offers an app to help women track their periods and pregnancies, and it boasts two hundred million users worldwide while being valued at eight hundred million dollars.[106] These services have become commonplace for women, and many rely upon them to stay informed about their menstrual cycles and general health. Similar apps to Flo state that medical researchers leverage anonymized data from these apps to examine women's health concerns.[107] In fact, some manufacturers assert that these apps include features intended to assist in diagnosing medical conditions.[108]

---

101. *Id.*

102. *Id.* (citation omitted).

103. *Id.*

104. *See generally* Emilie Smith, *Cycle-Tracking Apps and Data Privacy in the Post-Roe Climate*, MARQUETTE UNIV. LAW SCH. FAC. BLOG (Oct. 11, 2022), https://law.marquette.edu/facultyblog/2022/10/cycle-tracking-apps-and-data-privacy-in-the-post-roe-climate/ [https://perma.cc/NF2D-6X3L].

105. *See* Donna Rosato, *What Your Period Tracker App Knows About You,* CONSUMER REP. (Jan. 28, 2020), https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you-a8701683935/ [https://perma.cc/PT9F-TJKU].

106. *See* Emmy Lucas, *Women's Health App Flo Picks Up $50M in Fresh Funding to Fuel R&D, Rapid Growth*, FIERCE HEALTHCARE (Sep. 9, 2021), https://www.fiercehealthcare.com/digital-health/women-s-health-app-flo-closes-50m-series-b-funding-round-increases-valuation-to-800m [https://perma.cc/FP3W-QXUZ].

107. Rosato, *supra* note 105.

108. *Id.* Flo and Clue recently introduced tools to assess a user's risk of polycystic ovary syndrome, a hormone disorder that can affect a woman's fertility.

However, fitness bands and reproductive-related apps are not the only health apps when it comes to intimate data collection. Our bodies and the data associated with it are constantly under surveillance. Users who suffer from health issues are prone to rely on apps to monitor their bodies.[109] For example, customers suffering from migraines rely on apps such as Migraine Buddy[110] to track their migraine episodes, symptoms, triggers, and medications, and customers suffering from cancer rely on ChemoWave[111] to track their treatments. During the COVID-19 pandemic, there was a shift to users relying on mental health apps and telehealth services.[112] One telehealth app, GoodRx, sells health-related products including prescription discounts and telehealth services.[113] Despite promising its users that it would share their personal information with limited third parties and only for limited purposes, GoodRx was reported by the FTC for sharing sensitive user health data with third-party advertising companies and platforms, such as Google and Facebook.[114] In its complaint, the FTC stated that GoodRx allowed third parties that received a user's personal health information to use and profit from user data for their own business purposes.[115] As for the rise in popularity of mental health apps, a research team at Duke University's Sanford School of Public Policy examined how expansive the market for mental health data has become, explaining that many companies—in their own privacy policies—reserve the right to share data collected from their mental health

109. *See generally* Simon Usborne*, Intimate Data: Can a Person Who Tracks Their Steps, Sleep, and Food Ever Truly Be Free?,* THE GUARDIAN (Oct. 5, 2021), https://www.theguardian.com/lifeandstyle/2021/oct/05/intimate-data-can-a-person-who-tracks-their-steps-sleep-and-food-ever-truly-be-free [https://perma.cc/VR6B-AVTB].

110. Hannah Nichols & Stefano Lavarone, *Best Migraine Apps: 8 Options,* MED. NEWS TODAY (Oct. 19, 2022), https://www.medicalnewstoday.com/articles/319508 [https://perma.cc/2E58-E7N9].

111. Waverly Colville, *How One App Is Helping to Tighten the Link Between Cancer Patients and Their Doctors*, CNBC (Sep. 4, 2017), https://www.cnbc.com/2017/09/01/the-chemowave-app-feeds-data-from-cancer-patients-to-doctors.html [https://perma.cc/M3V7-KAEH].

112. JOANNE KIM, DATA BROKERS AND THE SALE OF AMERICANS' MENTAL HEALTH DATA: THE EXCHANGE OF OUR MOST SENSITIVE DATA AND WHAT IT MEANS FOR PERSONAL PRIVACY 2 (Feb. 2023) 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 [https://perma.cc/W4JG-PW7R]. Between 2019 and 2020, heath application downloads increased by 200%. *Id.*

113. Complaint for Permanent Injunction, Civil Penalties, and Other Relief at 2, United States. v. GoodRx Holdings, Inc., No. 23-cv-460 (N.D. Cal. Feb. 1, 2023).

114. *Id*.

115. *Id*. In a proposed order, filed by the DOJ on behalf of the FTC, GoodRx will be prohibited from sharing user health data with applicable third parties for advertising purposes and has agreed to pay a $1.5 million civil penalty for violating the rule. Press Release, Federal Trade Commission, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising [https://perma.cc/U989-9F7E].

apps with advertisers or other third-party partners.[116] Thus, health apps marketed to consumers collect and hand over large amounts of intimate health data without consumer protection safeguards in place.

B. Lack of HIPAA Protections for Intimate Health Data

Considering the sensitivity of the data collected by companies like GoodRx and mental health apps, it is counterintuitive for this data to not receive HIPAA protection.[117] Although many of these apps and services collect information that is normally stored by hospitals, HIPAA does not protect health data in all circumstances. HIPAA is a health care portability law, not a health privacy law.[118] The HIPAA Privacy Rule establishes a federal baseline for privacy protections that must be afforded to protected health information (PHI).[119] PHI refers to "individually identifiable" health information encompassing health data collected to identify an individual and determine appropriate care.[120] The HIPAA Privacy Rule only applies to PHI collected, used, or maintained by covered entities.[121] Currently, health data from most wearable devices, healthcare apps, and Internet of Things devices are not reviewed, collected, or maintained by a covered entity.[122] Instead, the day-to-day applications and devices consumers use involve gathering and retaining data that users willingly provide. This data is typically overseen by developers who do not meet the criteria as covered entities.[123] In the absence of a link to a covered entity, this data remains unprotected by HIPAA.

---

116. Drew Harwell, *Now For Sale: Data On Your Mental Health*, WASH. POST. (Feb. 13, 2023), https://www.washingtonpost.com/technology/2023/02/13/mental-health-data-brokers/ [https://perma.cc/3ECZ-LYGL].

117. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

118. CITRON, *supra* note 44, at 97.

119. Tawanna Lee & Antonio Reynolds, *All Data Is Not HIPAA Data- Healthcare Covered Entities Should Pay Close Attention to State Privacy laws Regulating the Health IoT Ecosystem*, JD SUPRA (July 13, 2021), https://www.jdsupra.com/legalnews/all-data-is-not-hipaa-data-healthcare-3523068/ [https://perma.cc/E3X9-5YD2].

120. *See Health Privacy: HIPAA Basics*, PRIV. RTS. CLEARINGHOUSE (Feb. 1, 2015), https://privacyrights.org/consumer-guides/health-privacy-hipaa-basics [https://perma.cc/3PQZ-Y37G].

121. *Id.*

122. Lee & Reynolds, *supra* note 119.

123. *Id.*

Data obtained from devices such as Fitbit, Apple Watch, sleep trackers, and other health-tracking apps have no legal protection under HIPAA.[124] Apps that store and interpret this data are also not given any special protection under HIPAA.[125] Clinton Mikel, a partner at Health Law Partners and a former chairman of the American Bar Association's eHealth, Privacy, and Security Interest Group, stated that "[t]he only things that cover [users] are the terms of service for Fitbit or Garmin or whomever, that frankly no one reads."[126]

Under the HIPAA Privacy Rule, covered entities cannot share medical record information because those records are defined as PHI.[127] However, data brokers can collect health-related data. Some data brokers specialize in aspects of intimate health data. For example, health data brokers can sell lists of rape victims, HIV and AIDS patients, and those suffering from erectile dysfunction and alcoholism.[128] For the low price of seventy-nine dollars, health brokers can sell a list of 1,000 names.[129] This means that for less than eight cents, anyone can access the intimate details of an individual's health.[130] Because selling this data contains the same level of sensitivity as data gathered by doctors and stored in hospitals, this poses a huge risk if it falls into the wrong hands.

C. Intimate Health Data Collection Risks for People Seeking Abortions

Collecting intimate health data creates potential harm that can be inflicted on various groups of people when this data is classified and traded with third-party data brokers. Because marginalized groups suffer greatly from underlying health issues, they are more likely to rely on

---

124. *See* Thomas Germain, *Guess What? HIPAA Isn't a Medical Privacy Law*, CONSUMER REP. (June 13, 2020), https://www.consumerreports.org/health-privacy/guess-what-hipaa-isnt-a-medical-privacy-law-a2469399940/ [https://perma.cc/Z28M-4MKC].

125. *Id*.

126. *Id.* (citation omitted).

127. *See generally The HIPAA Privacy Rule*, U.S DEP'T HEALTH AND HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/index.html#:~:text=The%20HIPAA%20Privacy%20Rule%20establishes,care%20providers%20that%20conduct%20certain [https://perma.cc/AKF5-SUQL] (last updated Mar. 31, 2022).

128. *See* Kashmir Hill, *Data Broker Was Selling Lists of Rape Victims, Alcoholics, and 'Erectile Dysfunction Sufferers*,' FORBES (Dec. 19, 2013), https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/?sh=747826601d53 [https://perma.cc/JQH4-SGFK].

129. *Id.*

130. *Id.*

services to monitor their health.[131] Therefore, the risk that accompanies the lack of protection of intimate health data is amplified for marginalized groups when this data is sold to the government. The concern of government surveillance of marginalized groups has long pre-dated the digital age. In the 1950s and 1960s, the government, in conjunction with the FBI's Counterintelligence Program, used surveillance programs to target Black Americans fighting against structural racism, which included Dr. Martin Luther King, Jr. and members of the Black Panther Party.[132] Even today, interested parties can collect and profit off of data at an unprecedented scale with minimal constraints.[133] This particularly concerns those who are seeking an abortion, as the collection of data puts these individuals at risk. After the decision in *Dobbs v. Jackson Women's Health Organization*,[134] this risk of government surveillance of health data will specifically impact those seeking abortions.

Data collection is and will be a major liability for people seeking abortions. With *Dobbs*[135] overturning the precedent set by *Roe v. Wade*,[136] individuals seeking abortions are put at risk by current unfettered data collection practices.[137] In *Dobbs*,[138] the United States Supreme Court struck down the right to abortion previously guaranteed by the U.S. Constitution, holding that the regulation of abortion is a matter for states to decide.[139] In *Dobbs*, a sole facility providing abortion services in Mississippi and one of its abortion providers brought an action against state officials responsible for overseeing health care and medical licensing.[140] The clinic challenged the constitutionality of Mississippi's Gestational Age Act, which prohibited abortions after fifteen weeks' gestation except in medical emergencies or in cases of severe fetal

131. *See* Nambi Ndugga & Samantha Artiga, *Disparities in Health and Health Care: 5 Key Questions and Answers*, KFF (Apr. 21, 2023), https://www.kff.org/racial-equity-and-health-policy/issue-brief/disparities-in-health-and-health-care-5-key-question-and-answers/#:~:text=Research%20shows%20that%20people%20living,the%20course%20of%20their%20lives [https://perma.cc/NR5D-S9AM].

132. *See* Samantha Lai & Brooke Tanner, *Examining the Intersection of Data Privacy and Civil Rights*, BROOKINGS INST. (July 18, 2022), https://www.brookings.edu/blog/techtank/2022/07/18/examining-the-intersection-of-data-privacy-and-civil-rights/ [https://perma.cc/HF7M-ZX6B].

133. *Id.*

134. 597 U.S. 215 (2022).

135. *Id.*

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

137. Lai & Tanner, *supra* note 132.

138. *Dobbs*, 597 U.S. at 215.

139. *See* Ellen Wright Clayton, Peter J. Embí & Bradley A. Malin, *Dobbs and the Future of Health Data Privacy for Patients and Healthcare Organization*s, 30 J. AM. MED. INFORMATICS ASSOC. 155 (2022).

140. *Dobbs*, 597 U.S. at 215.

abnormality.[141] The Court held that the U.S. Constitution does not confer a right to abortion,[142] overruling *Roe v. Wade*.[143] Many states will continue to protect the rights of pregnant individuals to make these essential healthcare decisions, but fourteen states have already enacted laws that severely limit or ban abortion altogether, with varying provisions from state to state.[144]

According to *Dobbs*, the state has a legitimate interest to act for the benefit of prenatal life "at all stages of development."[145] The Court claims that the rational basis test applies to any reproduction-related restriction and the state needs to show a "legitimate interest" to justify its actions.[146] Given this low legal standard of scrutiny, the Court nearly endorsed state action to protect prenatal life. The government has the power to monitor and control actions that could be considered risky to fetal health. After *Dobbs*, the government is now incentivized to track who decides to receive an abortion as well as any decision that pregnant people take to ensure that they are having a healthy child.[147] Accordingly, the most efficient way to track how millions of pregnant people are catering to their health can be accomplished through the purchase of health data.

With abortion bans in several states taking effect, prosecutors can investigate those seeking abortions.[148] This evidence may be collected from a wide array of application providers, communication networks, advertisers, and data brokers.[149] Intimate data points can be triangulated to reveal digital evidence related to abortions. For example, Fitbit data has been used to discredit a rape allegation,[150] indicating a trend toward prosecutors utilizing intimate data as evidence in trials.

---

141. *Id.*

142. *Id.* at 230.

143. *Id.*

144. *See* Mabel Felix, Laurie Sobel & Alina Salganicoff, *A Review of Exceptions in State Abortion Bans: Implications for the Provision of Abortion Services*, KFF (May 18, 2023), https://www.kff.org/womens-health-policy/issue-brief/a-review-of-exceptions-in-state-abortions-bans-implications-for-the-provision-of-abortion-services/ [https://perma.cc/9AVX-HBLD].

145. *Dobbs*, 597 U.S. at 301.

146. *Id.*

147. Leah R. Fowler & Michael R. Ulrich, *Femtechnodystopia*, 75 STAN. L. REV. 1233 (2022).

148. *See* Safia Samee Ali, *Prosecutors in States Where Abortion Is Now Illegal Could Begin Building Criminal Cases Against Providers*, NBC NEWS (June 24, 2022), https://www.nbcnews.com/news/us-news/prosecutors-states-abortion-now-illegal-begin-prosecute-abortion-provi-rcna35268 [https://perma.cc/Z4H5-34P6].

149. *Id.*

150. Jacob Gershman, *Prosecutors Say Fitbit Device Exposed Fibbing in Rape Case*, WALL ST. J. (Apr. 21, 2016), https://www.wsj.com/articles/BL-LB-53611 [https://perma.cc/S4SL-9HNW].

When it comes to women's health data, data privacy issues are exacerbated due to hyper-surveillance and an exorbitant amount of data collected related to "menstruation, fertility, pregnancies, menopause, pelvic and uterine health, nursing care, and sexual habits."[151] For the last three years, approximately one billion dollars has been invested in women's health technology.[152] However, this is not due to the tech industry becoming more aware of the needs of women.[153] In one study, researchers investigated the privacy practices of thirty menstruation-tracking apps.[154] The results of the study showed that reproductive-related data is not covered by privacy policies and disregarded—even when it is required for the apps to work.[155] Furthermore, the most popular female technology (FemTech) apps in the United States share user data with at least a half-dozen or more advertisers.[156]

These privacy risks are not limited to apps focused on reproductive management.[157] While period trackers are an obvious source of reproductive health data, experts suggest that other types of digital information are more likely to pose risks for women.[158] In 2020, Cynthia Conti-Cook, a civil rights lawyer and technology fellow at the Ford Foundation, published a paper on the digital evidence that prosecutors have used against pregnant people accused of feticide or endangering their fetuses.[159] Because this digital evidence includes anything from text messages to search history, this data is easily accessible.[160]

During trials and investigations, evidence collected from an individual's location data, text messages, and online activity have been

---

151. CITRON, *supra* note 44, at 30.

152. Kaitlyn Tiffany, *Period-Tracking Apps Are Not for Women*, VOX (Nov. 19, 2018), https://www.vox.com/the-goods/2018/11/13/18079458/menstrual-tracking-surveillance-glow-clue-apple-health [https://perma.cc/53NB-7DPF].

153. *Id.*

154. *See* Laura Schipp & Jorge Blasco, *How Private is Your Period? A Systematic Analysis of Menstrual App Privacy Policies*, 4 PROC. ON PRIV. ENHANCING TECHS. 491 (2020).

155. *Id.* Many apps request more data than disclosed in their privacy policies, with 56% requiring greater amounts than disclosed. *Id.* Notably, twenty-eight apps collect menstrual cycle data with fourteen transmitting it to servers, but only six apps explicitly mention this in their privacy policies. *Id.* Overall, there is inconsistency between privacy policy details and actual data requirements across these apps. *Id.*

156. CITRON, *supra* note 44, at 16.

157. Lai & Tanner, *supra* note 132.

158. *See* Kashmir Hill, *Deleting Your Period Tracker Won't Protect You*, N.Y. TIMES (June 30, 2022), https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html [https://perma.cc/EX7U-UJHE].

159. *Id.*

160. *Id.*

used by judges during convictions.[161] In June 2022, an investigation revealed that Facebook had been collecting data on individuals visiting the websites of crisis pregnancy centers.[162] If this data is packaged and sold by data brokers, government agencies may use this digital evidence without any proper safeguards. Internet searches could also be used to incriminate individuals. In 2017, lawyers used a Mississippi woman's online search for abortion drugs as evidence in a trial on the death of her fetus.[163] In 2015, a woman in Indiana was convicted based on text messages to a friend discussing taking abortion pills.[164] In that case, Purvi Patel was charged with felony child neglect and feticide, based on a supposed self-induced abortion.[165] Patel went to an emergency room in Indiana, and told the doctors she had a miscarriage.[166] When questioned about the fetal remains, Patel clarified that the baby was stillborn, prompting her to place the body in a bag and leave it in a dumpster due to her uncertainty about what to do.[167] Later, the government found text messages in which Patel told a friend she ordered and ingested pills to induce an abortion from a pharmacy in Hong Kong.[168] Patel then texted the same friend: "Just lost the baby."[169] Conti-Cook explained that "[t]hose text messages, those websites visited, [and] those Google searches are the exact type of intent evidence that prosecutors want to fill their bag of evidence."[170] Given these examples, it is clear that the government has been involved in investigating abortions as the government has an incentive to access any data that reveals intimate health information about consumers. In the absence of adequate safeguards, sensitive data may be vulnerable to exposure, granting the government unrestricted access to intimate health information.

---

161. Lai & Tanner, *supra* note 132.

162. *See* Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, REVEAL NEWS (June 15, 2022), https://revealnews.org/article/facebook-data-abortion-crisis-pregnancy-center/ [https://perma.cc/4GZ5-TME6].

163. *See* Geoffrey A. Fowler &Tatum Hunter, *For People Seeking Abortions Digital Privacy Is Suddenly Critical*, WASH. POST (May 4, 2022), https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/ [https://perma.cc/U2K4-7LEK]. The grand jury ultimately decided not to pursue charges. *Id.*

164. *See* Hill, *supra* note 158; *see also* Bazelon *infra* note 165.

165. Emily Bazelon, *Purvi Patel Could Be Just the Beginning*, N.Y. TIMES (Apr. 1, 2015), https://www.nytimes.com/2015/04/01/magazine/purvi-patel-could-be-just-the-beginning.html?partner=slack&smid=sl-share [https://perma.cc/DY8T-244H].

166. *Id.*

167. *Id.*

168. *Id.*

169. *Id.* (citation omitted).

170. Hill, *supra* note 158 (citation omitted).

III. THE LEGISLATIVE LANDSCAPE AND THE REGULATION OF GOVERNMENT COLLECTION OF INTIMATE DATA

Currently, the Fourth Amendment does not regulate the government's purchase of intimate health data from third-party data brokers.[171] However, there have been other legislative attempts to regulate how the government collects data on individuals broadly—the Privacy Act of 1974[172] and the Office of Management and Budget (OMB) Payment Integrity Information Act.[173] This section explains that, while these efforts attempt to protect intimate health data purchased by the government, they ultimately fall short.

A. Privacy Act of 1974

Prior to the rise of commercial data brokers, the Privacy Act of 1974 was passed to mitigate some of the concerns due to the computerization of personal records.[174] For example, computerization raised privacy concerns because of the broader scope of data being collected and the ease of accessing electronic records.[175] The Privacy Act applies to the federal government as well as government contractors.[176] Additionally, it limits the retention of nonessential data and First Amendment information that may be stored in electronic records.[177] However, the Privacy Act has been criticized for including too many exceptions, having a narrow application, and offering a limited scheme of remedies.[178] For example, the Privacy Act contains exemptions for systems of records maintained for law enforcement purposes.[179] Any general head of a federal agency such as the Secret Service or the Central Intelligence Agency may exclude a system of records from the reach of the Privacy Act.[180] Moreover, the Privacy Act contains a provision known as the "routine use" exception, which exempts records collected for a purpose that aligns with the original

171. Rahbar, *supra* note 30, at 713.

172. 5 U.S.C. § 552(a).

173. Pub. L. No. 116-117, 133 Stat. 31 (2019).

174. *See* James McCain, *Applying the Privacy Act of 1974 to Data Brokers Contracting with the Government*, 38 PUB. CONT. L. J. 935, 936 (2009).

175. *Id.*

176. *Id.* at 939.

177. *Id.* at 938–39.

178. *Id.* at 939.

179. *Id.* at 940.

180. *Id.*

purpose of collection.[181] For example, information gathered by the FBI could be shared with another agency, so long as the agency plans to use the information for law enforcement purposes.[182] The process is as simple as submitting a written request specifying its desired portion of the record and the relevant law enforcement activity.[183] Accordingly, these exemptions leave federal agencies with a lot of discretion in sharing and storing data, allowing them to do so without rigorous oversight regarding the types of data collected and its intended purpose. This can create problems as the Privacy Act applies to U.S. agencies such as the Internal Revenue Service, the Department of Health and Human Services, the Social Security Administration, the Department of Homeland Security, federal law enforcement agencies, and more.[184]

Therefore, the Privacy Act touches on a *true* privacy concern: preventing the U.S. government from becoming an "unchecked database" that purchases data and stores it without regulation.[185] However, the law is outdated. Federal agencies maintain vast amounts of personal data, leveraging that data to make decisions that can profoundly impact the lives of users. Thus, the American public deserves better privacy protections from the government than the loose protections stemming from a nearly fifty-year-old law.

B. The Office of Management and Budget: Payment Integrity Information Act

The Office of Information and Regulatory Affairs, a branch within the Office of Management and Budget (OMB), is responsible for overseeing the implementation of the Privacy Act of 1974 across federal agencies.[186] Despite this oversight, federal agencies have long evaded the privacy

---

181. *Id.* at 936; *see also* Christopher W. Wasson, *Privacy Law- The Routine Use Exception to the Privacy Act: A Clarification on Compatibility,* 35 VILL. L. REV. 822, 823 (1990). Before an agency invokes this exception, it has to have previously published a list of routine uses with the Federal Register. *Id.* An agency has to meet a published routine use in order to justify an unauthorized disclosure. *Id.*

182. McCain, *supra* note 174.

183. LINEBAUGH, *supra* note 17, at 4.

184. *See generally Overview of The Privacy Act of 1974*, U.S. DEP'T OF JUST., https://www.justice.gov/archives/opcl/definitions#:~:text=%E2%80%9Cany%20Executive%20department%2C%20military%20department,independent%20regulatory%20agency.%E2%80%9D%205%20U.S.C [https://perma.cc/2ZNA-S7BS].

185. 5 U.S.C. § 552(a).

186. Information and Regulatory Affairs, *Privacy*, WHITE HOUSE, https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/#:~:text=Among%20other%20things%2C%20OIRA%20is,Act%20of%201974%205%20U.S.C. [https://perma.cc/9H4V-2NQU].

standards in the Privacy Act by using information from third-party data brokers.[187]

Specifically, the OMB issues guidance and regulations to federal agencies to help them comply with the Privacy Act. For example, the OMB issued a memorandum in 2010 that provides guidance for agency uses of third-party websites.[188] The memo requires federal agencies to "take specific steps to protect individual privacy whenever they use third-party websites or applications to engage with the public."[189] Among other requirements, the memo directs agencies to create a tailored Privacy Impact Assessment that addresses the specific functions of a third-party website or application in use.[190] However, these guidelines are non-binding and only set out norms for agencies to follow.[191]

In 2013, the OMB set out the Do Not Pay (DNP) policy in order to take a proactive step in limiting the federal government's abuse of data brokers.[192] The DNP policy is authorized and governed by the Payment Integrity Information Act of 2019.[193] The DNP policy states that:

> The OMB memo requires agencies involved in the [DNP] Initiative to apply privacy standards for evaluating the use of commercial databases with personal information. The standards themselves are not new. They are the same standards that federal agencies have complied with for the nearly forty years that the Privacy Act of 1974 has been in place. What is new is that the standards will apply externally to commercial services and

187. ROBERT GELLMAN & PAM DIXON, WORLD PRIV. F., DATA BROKERS AND THE FEDERAL GOVERNMENT: A NEW FRONT IN THE BATTLE FOR PRIVACY OPENS 4 (Oct. 30, 2013), https://www.worldprivacyforum.org/2013/10/report-data-brokers-and-government-introduction-and-background/ [https://perma.cc/Q5G8-AXS2].

188. *See* OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, OMB MEMO. M-10-23, GUIDANCE FOR AGENCY USE OF THIRD PARTY WEBSITES AND APPLICATIONS (2010), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf [https://perma.cc/76EC-E6AY].

189. Memorandum from Kevin Neyland, Deputy Adm'r, Off. of Info. and Regul. Affs. to the Federal Chief Information Officers, Model Privacy Impact Assessment for Agency Use of Third-Party Websites (Dec. 29, 2011), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/inforeg/inforeg/info_policy/model-pia-agency-use-third-party-websites-and-applications.pdf [https://perma.cc/4HDG-3XMJ].

190. *Id.* at 4.

191. *See* KATE BOWERS, CONG. RSCH. SERVS., AGENCY USE OF GUIDANCE DOCUMENTS (1st ed. 2021), https://www.everycrsreport.com/files/2021-04-19_LSB10591_9477746a9161f3ee6f2d127a70eb84cdcec6e4df.pdf [https://perma.cc/4247-TUL8].

192. GELLMAN & DIXON, *supra* note 187, at 15.

193. *Do Not Pay*, BUREAU OF THE FISCAL SERV. U.S. DEP'T OF TREASURY, https://fiscal.treasury.gov/DNP/#:~:text=DNP%20is%20authorized%20and%20governed,the%20Department%20of%20the%20Treasury [https://perma.cc/6NBA-TT7H].

> databases provided to the government and not just internally to government activities or information that the government maintains . . . . The [DNP] Initiative seeks to curb waste and fraud in the federal government by limiting, reviewing, and verifying information to identify inappropriate federal agency payments.[194]

The DNP policy encompasses information within commercial databases used in the DNP Initiative—including The Work Number[195]—requiring up-to-date and accurate information to uphold fairness to the individuals featured in those records.[196] In addition, the Privacy Act of 1974 governs the DNP Initiative in the handling of data, to safeguard records that include an individual's personal identifiers such as names, social security numbers, or other identifying numbers or symbols.[197] In 2021, the OMB released a memorandum to ensure that individual privacy is fully protected while reducing improper payments with the DNP Initiative.[198] However, the DNP Initiative only applies to databases used in the policy, and the majority of data brokers are not included in those databases.[199] Furthermore, most intimate health data exists outside the databases of the DNP Initiative.

There are still significant loopholes remaining in the OMB guidance. For example, the federal government is adopting a "data outsourcing" model that allows the government to evade Privacy Act protections by purchasing data from data brokers.[200] Despite the existence of the Privacy Act and OMB guidance, consumer health data is inadequately protected and susceptible to federal government surveillance. This underscores the outdated nature of the Privacy Act, which fails to prevent the government from purchasing consumer data.

---

194. GELLMAN & DIXON, *supra* note 187 (emphasis removed).

195. *Id.* This report expands on the Work Number and states:

> The Work Number is part of Equifax, one of the leading credit bureaus. The Work Number database is said to contain information on more than 190 million Americans, with as many as 12 million added each year. Information from The Work Number is sold to debt collectors, financial service companies, and other entities. Equifax says that employment verification information (that is, where you work, but not specific pay information) is only sold to debt collectors with consent, as required by the Fair Credit Reporting Act.

Id. at 10 (emphasis removed) (citations omitted).

196. *Id.* at 5.

197. *See Do Not Pay Privacy Program*, BUREAU OF THE FISCAL SERV. U.S. DEP'T OF TREASURY, https://fiscal.treasury.gov/dnp/privacy-program.html [https://perma.cc/B3W7-776P].

198. *See* OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, OMB MEMO. M-21-19, APPENDIX C: REQUIREMENTS FOR PAYMENT INTEGRITY IMPROVEMENT (2021), https://fiscal.treasury.gov/files/dnp/M-21-19.pdf [https://perma.cc/SJ5B-BQA5].

199. GELLMAN & DIXON, *supra* note 187, at 16.

200. *Id.* at 5.

C. Current Legislative Reform Attempts: Fourth Amendment Is Not For Sale Act

The current legal landscape is inadequate to address the government's ability to purchase intimate health data from third-party data brokers. Alongside the outdated Privacy Act of 1974, the United States does not have a comprehensive federal privacy law. Most legislative attempts are focused on protecting consumer information from intrusive collection by private companies. For example, state privacy laws such as Washington's My Health My Data Act[201] or Illinois' Biometric Information Privacy Act[202] establish standards for how companies handle consumer health information. However, these laws only apply to private companies, not to the federal government.

There are growing concerns about the collection, use, and sale of personal data by third-party data brokers, and the potential for government agencies to purchase and use this data for surveillance and law enforcement purposes without appropriate safeguards and oversight. In response to these concerns, lawmakers have proposed various legislative reforms to provide stronger protections for personal data in the digital age, such as the Fourth Amendment Is Not For Sale Act.[203]

In 2021, Senator Ron Wyden, along with eighteen other senators, proposed the Fourth Amendment Is Not For Sale Act.[204] This bill, whose co-sponsors include Senators Rand Paul and Bernie Sanders, would require the government to obtain court orders before compelling data brokers to disclose personal user data.[205] This bill was proposed in response to concerns about the collection, use, and sale of personal data by data brokers and the potential for government agencies to purchase and use this data for surveillance and law enforcement purposes without a warrant.[206] In July 2023, the proposed bill passed through the House Judiciary Committee.[207]

---

201. 2023 Wash. Sess. Laws 191.

202. 740 ILL. COMP. STAT. 14 (2008).

203. Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. (2021).

204. *Id.*; *see also* Press Release, Ron Wyden, Wyden, Paul and Bipartisan Members of Congress Introduce the Fourth Amendment Is Not For Sale Act (Apr. 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act- [https://perma.cc/L3BT-UMV4].

205. *See* Press Release, Wyden, *supra* note 204.

206. *Id.*

207. Press Release, Warren Davidson, Fourth Amendment Is Not For Sale Act Passes Judiciary Committee (July 19, 2023), https://davidson.house.gov/2023/7/fourth-amendment-is-not-for-sale-act-passes-judiciary-committee [https://perma.cc/4HTQ-AYXZ].

This bill aims to close the legal loophole that enables data brokers to sell the personal information of Americans to law enforcement without judicial oversight.[208] The government's ability to purchase data stands in contrast to the rigorous regulations that phone companies, social media sites, and other consumer-facing businesses must adhere to.[209] Speaking on the importance of this bill, Senator Wyden stated: "I don't think Americans' Constitutional rights ought to vanish when the government uses a credit card instead of a court order."[210]

Under this bill, the Storage Communications Act (SCA) would be amended to treat data brokers like other providers, where the government would need a form of court approval when it wants to purchase information from data brokers.[211] More specifically, the bill aims to prevent law enforcement agencies from bypassing the *Carpenter* warrant process by purchasing data from third-party data brokers.[212] Additionally, the bill encompasses provisions to prevent government agencies from indirectly acquiring records and information from third parties, while also prohibiting the sharing of information between non-law enforcement or between intelligence agencies and law enforcement.[213]

The Fourth Amendment Is Not For Sale Act has garnered significant support. On January 26, 2022, the Brennan Center for Justice, a highly regarded non-partisan law and policy institute, together with nearly fifty organizations dedicated to privacy rights, governmental transparency, and surveillance reform, collectively urged for congressional action on the Fourth Amendment Is Not For Sale Act.[214] In this letter, the Center highlighted that "relevant federal statutes were written at a time when apps and digital brokers did not exist . . . . As a result, data from apps most Americans routinely use are open to warrantless examination by the government."[215] Furthermore, in July 2022, at a hearing hosted by the

208. *See* Press Release, Wyden, *supra* note 204.

209. *Id.*

210. Nilay Patel & Adi Robertson, Donald Trump Trying to Control the FCC Is a 'Disaster,' Says Sen. Ron Wyden, THE VERGE (Aug. 4, 2020), https://www.theverge.com/2020/8/4/21354244/ron-wyden-fcc-nomination-section-230-trump-order-vergecast-interview [https://perma.cc/XC5R-AQ89] (quoting Interview with Ron Wyden, U.S. Senator for Or. (Aug. 4, 2020)).

211. BALSER, *supra* note 27, at 3.

212. Isabelle Canaan, *A Fourth Amendment Loophole?: An Exploration of Privacy and Protection Through the Muslim Pro Case*, COLUM. HUM. RTS. L. REV. 96, 118 (2022).

213. *Id.* at 118–19.

214. *See Coalition Letter Calls for Congressional Hearings on Fourth Amendment Is Not For Sale Act*, BRENNAN CTR. FOR JUST. (Jan. 26, 2022), https://www.brennancenter.org/our-work/research-reports/coalition-letter-calls-congressional-hearings-fourth-amendment-not-sale [https://perma.cc/S5SZ-JB64].

215. *Id.*

House Judiciary Committee titled "Digital Dragnets: Examining the Government's Access to Your Personal Data," representatives expressed broad bipartisan consensus for the bill.[216]

This bill still faces a lengthy legislative process, prompting state legislatures to introduce various initiatives aimed at enhancing the protection of consumer data. For example, in 2019, Utah legislators voted unanimously to pass the Electronic Information or Data Privacy Act.[217] This Act states that, for investigation or prosecution, "a law enforcement agency may not obtain, without a search warrant issued by a court upon probable cause [the] location information, stored data, or transmitted data" or "electronic information or data transmitted by the owner of the electronic information or data to a remote computing service provider."[218] This Act thus indicates the growing desire to regulate law enforcement access to consumer data when there are currently no federal laws that regulate the government's access to intimate health data.

IV. PROPOSED LEGISLATIVE SOLUTIONS

The enactment of the Fourth Amendment Is Not For Sale Act is crucial because the current hands-off approach to consumer health technologies has created conditions that leave consumer health data and third-party data brokers operating in an unregulated ecosystem. Consequently, government entities are incentivized to purchase and analyze data without permission, circumventing Fourth Amendment protections through financial means. In the absence of oversight, federal agencies use purchased data to target vulnerable communities. Disturbingly, the U.S. government is one of the largest and most frequent customers of commercial data brokers.[219] Instead of creating its own databases subject to privacy laws applicable to federal agencies, the federal government often outsources the collection of intimate data to data brokers, as privacy laws do not apply to these entities.[220] Commercial data brokers have thus long been employed for government law enforcement purposes in this capacity.[221]

---

216. Justin Hendrix, *Bipartisan Support for Fourth Amendment Is Not For Sale Act at House Judiciary Hearing*, TECH POL'Y PRESS (July 19, 2022), https://techpolicy.press/bipartisan-support-for-fourth-amendment-is-not-for-sale-act-at-house-judiciary-hearing/ [https://perma.cc/MJ45-D3DM] (emphasis removed).

217. Electronic Information or Data Privacy Act, H.B. 57, 2019 Leg. Gen. Sess. (Utah 2019) https://le.utah.gov/~2019/bills/static/HB0057.html [https://perma.cc/8FG8-B48W].

218. *Id.*

219. GELLMAN & DIXON, *supra* note 187, at 4.

220. *Id.*

221. *Id.*

Largely, lawmakers have left consumers to fend for themselves and are relying on those consumers to opt-out of companies collecting their data by doing their own research. If every consumer was informed on how much of their own data was being kept and sold, today's privacy problems would be significantly reduced. However, to do so logically would mean that consumers would have to read all the privacy policies on the websites they visit. A research study conducted at Carnegie Mellon revealed that if each internet user were to meticulously read the privacy policy on every website visited, they would spend a staggering twenty-five days per year solely dedicated to reading privacy policies.[222] It would be impractical to place the burden on consumers to single-handedly ensure that private companies refrain from selling information to third-party data brokers or to ascertain whether the government is procuring their data through these brokers.

Although consumer education and information collection transparency could assist users in making informed decisions about data-sharing settings on their devices, users will continue to look to other sources to create data protections for their intimate health information. While the FTC may bring enforcement actions against companies that collect intimate health data, consumers need proactive legislation to regulate the government's purchase and use of this data. Existing legislation, such as the Privacy Act of 1974, the ECPA, and the OMB guidance have so far been insufficient in protecting a user's intimate health data from government purchases. This Comment argues that separate legislation regulating the government's purchase of intimate health data is needed. Therefore, Congress should pass the Fourth Amendment Is Not For Sale Act.[223] In doing so, this Comment seeks to amend the proposed bill so that it contains explicit provisions related to intimate health data.

A. Proposed Reforms to the Fourth Amendment Is Not For Sale Act

As discussed above, the Fourth Amendment does not prohibit the government's purchase of intimate health data.[224] In the wake of *Dobbs*, consumers should be more concerned than ever that data related to their bodies can be triangulated, de-anonymized, and used as a surveillance

222. Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ [https://perma.cc/ZB4G-HCBX].

223. Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. (2021).

224. LINEBAUGH, *supra* note 17, at 2.

mechanism by government agencies.[225] Currently, law enforcement and intelligence agencies can generally buy sensitive health data from data brokers without a warrant.[226] Law enforcement and intelligence agencies at all levels of government are purchasing this data for their own use, circumventing safeguards designed to restrict direct acquisition of the exact same information. This practice bypasses the *Carpenter* warrant requirements imposed on law enforcement requests for consumer data from third-party providers.[227]

The Fourth Amendment Is Not For Sale Act does not encompass enough. Although the goal is to regulate data brokers' ability to sell Americans' personal information to law enforcement and intelligence agencies without any court oversight, the bill needs to be reformed in two respects. First, the bill must mention and define health data. Second, the bill must establish measures to prohibit the government from buying or using intimate health data. Specifically, the bill needs to address government purchasing of data from companies using misleading privacy policies to obtain consumer consent in order to share collected health data.

For the first reformation, the bill's objectives specifically mention and emphasize the importance of protecting location data—not user health data.[228] Section (e)(2)(A) states, "A . . . governmental entity . . . may not obtain from a third party in exchange for anything of value a covered customer or subscriber record or any illegitimately obtained information."[229] The bill defines a "covered record" as a record or other information that pertains to a covered person or is the contents of a communication or location information.[230] Specifically, the bill needs to add a provision to clarify that covered records include the health data that pertains to a covered person.

In addition, the bill could benefit from echoing the definition of consumer health data provided in the Washington My Health My Data Act.[231] This Act defines consumer health data as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."[232] Physical or mental health status includes: individual health conditions, treatment, diseases, or diagnoses, health-related surgeries or

225. Clayton et al., *supra* note 139, at 155.

226. LINEBAUGH, *supra* note 17, at 2.

227. Carpenter v. United States, 585 U.S. __,138, S. Ct. 2206 (2018).

228. S. 1265.

229. *Id.* § 2(e)(2)(A).

230. *Id.* § 3(e)(1)(C).

231. 2023 Wash. Sess. Laws 191.

232. *Id.* § 3(8)(a).

procedures, use or purchase of prescribed medication, bodily functions, vital signs, symptoms, diagnoses or diagnostic testing, treatment, or medication, gender-affirming care information, reproductive or sexual health information, biometric and genetic data, precise location information that may indicate a consumer's intent to seek health services, and data that identifies a consumer seeking health care services, derived from non-health information.[233] Similar to the Washington My Health My Data Act, the Fourth Amendment Is Not For Sale Act should include a holistic definition of consumer health data to ensure the protection of personal and private aspects of consumers' lives.

The bill explicitly protects information that, if combined with other data, could be used to identify an individual.[234] It is imperative to tackle this issue in order to safeguard an individual's privacy. As the volume and granularity of data collected through diverse media platforms and apps continue to surge, a tangible threat emerges: the government may aggregate and cross-reference these data points, constructing a comprehensive profile of an individual. In doing so, they might effectively de-identify individuals, erasing the thin veil of anonymity that is often assumed to protect personal information. The government should ensure that any data it collects is necessary, proportional, and subject to appropriate safeguards. Additionally, the government should use de-identified data only when a warrant allows for it.

Furthermore, the bill includes a detailed definition of third parties and explicitly states that no governmental entity may obtain a covered customer's record from a third party in exchange for anything of value.[235] In order to ensure that governmental entities are not circumventing the Fourth Amendment, the bill notably states that "[u]nless a governmental entity obtains an order in accordance [with the bill], the governmental entity may not require a third party to disclose a covered customer or subscriber record or any illegitimately obtained information if a court order would be required for the governmental entity [to obtain the information]."[236] While this provision is a step in the right direction, this Comment urges lawmakers to include an additional provision that explicitly provides this protection to intimate health data within the meaning of a covered record, much like it has for location data.[237]

233. *Id.* § 3(8)(b).

234. S. 1265.

235. *Id.*

236. *Id.*

237. *See id*. § (2)(e)(1)(C)(ii)(III).

For the second reformation, when looking at section (e)(2)(A),[238] this bill needs to consider situations where a privacy policy could include hidden language that allows a company to sell data to a data broker, which, in turn, allows the government to openly access and purchase this data.[239] The bill's definition of "illegitimately obtained information" needs to include a section that expands on what it means to "deceive the covered person" and to require "opt-in consent" for consumers who are using applications and devices that collect health data.[240] For example, the Apple Watch privacy policy claims they are committed to their users' privacy.[241] However, the privacy settings are designed in a manner that requires users to navigate through several complex steps to secure their data. In order to check which services are linked to their Apple Watch, users have to check the "permissions" screen on the watch settings.[242] These permissions allow the app to take and use data from Apple Health.[243] Users can choose to disable permissions, disconnect the app entirely, and delete the data shared with Apple Health.[244]

There is also a gap in the language of the Fourth Amendment Is Not For Sale Act. Without mandating opt-in consent or explicitly defining that "deceiving" a covered person includes subjecting them to intricate steps to opt-out of data sharing, the efficacy of the bill in protecting consumers may be compromised.[245] To illustrate this, without requiring opt-in consent, the bill allows data collected by the Apple Watch—such as blood oxygen levels or heart rates—to be shared with a third-party service connected to the user's Apple Watch, unless the user actively checks the "permissions" page to disable data sharing.[246] Many users tend to skip over privacy policies and do not thoroughly review them, which means

---

238. *Id.*

239. *See Your Data Is Shared And Sold…What's Being Done About It?*, KNOWLEDGE AT WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/HT59-RB2N].

240. S. 1265 § 2(e)(1)(E).

241. *See generally Health Privacy Overview*, APPLE (May 2023), https://www.apple.com/privacy/docs/Health_Privacy_White_Paper_May_2023.pdf [https://perma.cc/G7PQ-XM45].

242. David Nield, *How to Lock Down Your Health and Fitness Data*, WIRED (Nov. 17, 2019), https://www.wired.com/story/health-fitness-data-privacy/ [https://perma.cc/HQ6S-7X97].

243. *Id.* Apple Health is the health app that gathers health data from a user's iPhone, iPad, or Apple Watch, acting as a centralized hub for all a user's health data. *See* Apple Support, *Use the Health App on Your iPhone or iPad*, APPLE (Nov. 28, 2023), https://support.apple.com/en-us/104997#:~:text=The%20Health%20app%20gathers%20health,automatically%20tracks%20your%20Activity%20data [https://perma.cc/JLT9-7F43].

244. Nield, *supra* note 242.

245. S. 1265 § 2(e)(1)(E).

246. *See* Nield, *supra* note 242.

they may inadvertently permit such data sharing. For example, if a user does not opt-out, the data is not "illegitimately obtained information."[247] If the user authorized this information and technically consented to it, then the data was not collected, processed, or shared in violation of a contract related to the Apple Watch user. Under the existing proposed bill, government acquisition of this data is justified even if the user is entirely uninformed regarding the utilization of their health data.

To rectify this, there should be greater oversight of data brokers and government agencies that obtain data from them. This includes requiring data brokers to register with the OMB database and submit to regular audits and inspections in order to ensure compliance with privacy laws. Government entities should only be allowed to purchase data from pre-approved data brokers with a valid court order or warrant. Also, the Fourth Amendment Is Not For Sale Act needs to explicitly call for increased transparency about the kind of data the government is purchasing. Government agencies should be required to disclose how they obtain data from companies and what they choose to do with it. This transparency will help ensure that the government is not engaging in backdoor surveillance by purchasing intimate health data without legal oversight.

CONCLUSION

The government's ability to purchase intimate health data from data brokers without a warrant raises significant concerns because it infringes upon an individual's privacy and bodily autonomy. Given the sensitive nature of intimate health data, there is a compelling need for more robust regulations on how data is used and who has access to it. This Comment explored how the government's purchase of intimate health data from third-party data brokers circumvents the Fourth Amendment's protections against unreasonable searches and seizures. Specifically, this Comment analyzed how purchasing intimate health data creates risks for groups that are highly surveilled and monitored by the government, such as those seeking abortions. In response to these concerns, this Comment urges lawmakers to pass the Fourth Amendment Is Not For Sale Act and offers recommendations for reforming the proposed bill. The suggested reforms include opt-in consent requirements and explicit provisions defining intimate health data, ensuring that the legislation adequately addresses the unique challenges posed by the acquisition of health data. Additionally, there is a need for increased oversight of data brokers to ensure

247. S. 1265 § 2(e)(1)(E).

compliance with existing laws, such as requiring registration with the OMB database as well as conducting regular audits and inspections. In an era characterized by pervasive data collection in an unregulated ecosystem, comprehensive legislation is needed to safeguard consumers against the selling of intimate health data.