RUTGERS JOURNAL OF LAW & PUBLIC POLICY

About the Rutgers Journal of Law & Public Policy

The *Rutgers Journal of Law and Public Policy* (ISSN 1934-3736) is published two times per year by students of the Rutgers School of Law – Camden, located at 217 North Fifth Street, Camden, NJ 08102.

Form: Citations conform to The Bluebook: A Uniform System of Citation (21st ed. 2021).

Please cite the Rutgers Journal of Law & Public Policy as 20 RUTGERS J.L. & PUB. POL'Y __ (2023).

Manuscripts: The *Rutgers Journal of Law & Public Policy* seeks to publish articles making original contributions in the field of public policy. The Journal accepts both articles and compelling essays for publication that are related to the expansive topic of public policy. Manuscripts must contain an abstract describing the article or essay which will be edited and used for publication on the website and in CD-ROM format. The Journal welcomes submissions from legal scholars, academics, policy makers, practitioners, lawyers, judges and social scientists.

Electronic submissions are encouraged. Submissions by email and attachment should be directed to submissions.rjlpp@gmail.com.

Paper or disk submissions should be directed to *Rutgers Journal of Law & Public Policy*, Rutgers University School of Law – Camden, 217 North Fifth Street, Camden, New Jersey 08102.

Subscriptions: Subscription requests should be mailed to *Rutgers Journal of Law & Public Policy*, Rutgers University School of Law – Camden, 217 North Fifth Street, Camden, New Jersey 08102, or emailed to info@rutgerspolicyjournal.org.

Internet Address: The *Rutgers Journal of Law & Public Policy* website is located at http://www.rutgerspolicyjournal.org.

RUTGERS, THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS LAW SCHOOL

OFFICERS OF THE UNIVERSITY

JONATHAN HOLLOWAY, A.B., M.A., M.Phil., Ph.D., *President of the University*
NANCY CANTOR, A.B., Ph.D., *Chancellor of Rutgers University—Newark and Distinguished Professor*
ANTONIO D. TILLIS, B.A., M.A., Ph.D., *Chancellor of Rutgers University—Camden and Professor of Law*
DANIEL HART, B.A., Ed.D., *Provost of Rutgers University—Camden and Professor and Executive Vice Chancellor*
ASHWANI MONGA, B.TECH., M.B.A, Ph.D., *Provost of Rutgers University—Newark and Executive Vice Chancellor*

JOHANNA BOND, B.A., J.D., *Dean and Professor of Law*
SHANI KING, B.A., J.D., *Vice Dean and Professor of Law*
ARTHUR LABY, B.A., J.D., *Vice Dean and Professor of Law*
VICTORIA CHASE, B.A., J.D., *Associate Dean for Academic Affairs, Associate Clinical Professor of Law*
RONALD CHEN, B.A., J.D., *Associate Dean for Academic Affairs, Associate Professor*
NANCY TALLEY, B.A., M.S., J.D., *Senior Associate Dean for Information Services*
CAROLINE YOUNG, B.A., J.D., *Senior Associate Dean for Information Services*
JON C. DUBIN, A.B., J.D., *Associate Dean for Clinical Education and Board of Gov. Dist. Public Service Professor of Law*
WEI FANG, B.S., M.L.I.S., M.S.C.S., *Associate Dean for Information Technology and Head of Digital Services*
JILL FRIEDMAN, B.A., J.D., *Associate Dean of Pro Bono & Public Interest and Professor of Law*
ELLEN P. GOODMAN, A.B., J.D., *Associate Dean of Strategic Initiatives & Special Projects and Professor of Law*
VANESSA WILLIAMS, B.A., Ph.D., *Assistant Dean of New Programs*
SUZANNE KIM, B.A., J.D., *Associate Dean of Academic Research Centers and Professor of Law*
DAVID NOLL, B.A., J.D., *Associate Dean for Faculty Research and Development and Professor of Law*
SARAH K. REGINA, B.A., J.D., *Associate Dean for Student Affairs*
ANDREW ROSSNER, B.A., M.A., J.D., *Associate Dean for Professional & Skills Education and Distinguished Professor of Law*
ROBERT STEINBAUM, B.A., J.D., *Associate Dean for Advancement*
AMY MILLER, B.A., J.D. Ed.D., MSEd, *Associate Dean of Students Affairs*
SARAH K. REGINA, B.A., J.D, *Associate Dean of Students Affairs*
ELIZABETH ACEVEDO, B.S., J.D., *Assistant Dean for Career Development*
CLIFFORD DAWKINS, B.A., J.D., *Assistant Dean, Minority Student Program*
RHASHEDA DOUGLAS, B.A., J.D., *Assistant Dean, Minority Student Program*
SUSAN FEATHER, B.A., M.A., J.D., *Assistant Dean for Public Interest and Pro Bono*
LINDA GARBACCIO, B.S., *Assistant Dean for Academic Services*
MATTHEW SALEH, B.A., J.D., Ph.D., *Assistant Dean of Admissions*
ROBIN L. TODD, B.A., *Assistant Dean for Development*
REBEKAH VERONA, B.S., J.D., *Assistant Dean for Career Development*
JEFFREY BALOG, *Director of Finance and Administration*
JOANNE GOTTESMAN, B.A., J.D., *Director of Clinical Programs and Clinical Associate Professor*
JOHN C. LORE, III, B.A., J.D., *Director of Trial Advocacy and Distinguished Clinical Professor of Law*
Margaret McCarthy, *Director of Communications and Marketing*
PAM MERTSOCK-WOLFE, B.A., M.A., *Director of Pro Bono and Public Interest*
ELIZABETH MOORE, B.A., *Director of Communications*
THOMAS RYAN, *Director of Information Technology*
CAROL WALLINGER, B.S., J.D., *Director of Lawyering and Clinical Professor of Law*

Professors of Law Emeriti

Frank Askin, B.A., J.D.,
Distinguished Professor of Law Emeritus, Robert E. Knowlton Scholar, and Director of the Constitutional Rights Clinic
Paul Axel-Lute, B.A., M.L.S.,
Deputy Director of the Law Library Emeritus
Cynthia A. Blum, B.A., J.D.,
Professor of Law Emerita
A Hays Butler, B.A., J.D., M.S. (LIS),
Law Librarian Emeritus
Norman L. Cantor, A.B., J.D.,
Professor of Law Emeritus
Edward E. Chase, B.A., J.D.,
Professor of Law Emeritus
Roger S. Clark, B.A., LL.B., LL.M., J.S.D., L.L.D.,
Board of Governors Professor and Distinguished Professor of Law Emeritus
Russell M. Coombs, B.A., J.D.,
Professor of Law Emeritus
Lucy Cox, B.A., M.S., Ph.D., M.L.S., *International & Foreign Law Librarian Emerita*
Anne V. Dalesandro, A.B., M.L.S., J.D.,
Law Library Director Emerita and Professor of Law Emerita
John H. Davies, B.S., LL.B., LL.M.,
Professor of Law Emeritus
Stuart L. Deutsch, B.A., J.D., LL.M., *University Professor and Willard Heckel Scholar*
Jack Feinstein, B.A., J.D.,
Clinical Professor of Law Emeritus
George Ginsburgs, B.A., M.A., Ph.D.,
Distinguished Professor of Law Emeritus
Arno Liivak, B.A., M.L.S., J.D.,
Professor of Law Emeritus
Jonathan Mallamud, A.B., J.D.,
Professor of Law Emeritus
Craig N. Oren, A.B., J.D.,
Professor of Law Emeritus
James Gray Pope, A.B., J.D., Ph.D.,
Distinguished Professor of Law and Sidney Reitman Scholar
Patrick J. Ryan, B.A., M.A., J.D., LL.M., J.S.D.,
Associate Professor of Law Emeritus
Carol Roehrenbeck, B.A., M.L.S., J.D.,
Professor of Law and Director of the Law Library Emerita
Rand E. Rosenblatt, B.A., M.Sc., J.D.,
Professor of Law Emeritus
Diana Sclar, B.A., J.D.,
Professor of Law
Peter Simmons, A.B., LL.B.,
University Professor Emeritus and John M. Payne Scholar
Richard G. Singer, B.A., J.D., LL.M., J.S.D.,
Distinguished Professor of Law Emeritus
E. Hunter Taylor, B.A., LL.B., LL.M.,
Professor of Law Emeritus
Paul L. Tractenberg, B.A., J.D.
Board of Governors Distinguished Service Professor and Professor of Law
Robert M.Washburn, A.B., J.D., LL.M,
Professor of Law Emeritus
Robert F. Williams, B.A., J.D., LL.M.,
Distinguished Professor of Law Emeritus

Faculty of Law

Aaron Ari Afilalo, A.B., J.D., LL.M.,
Professor of Law
Charles Auffant, B.A., J.D.,
Clinical Professor of Law
Sahar Aziz, B.SC., M.A., J.D.,
Professor of Law
Carlos A. Ball, B.A., J.D., LL.M.,
Distinguished Professor of Law
Bernard W. Bell, B.A., J.D.,
Professor of Law
Vera Bergelson, J.D., Ph.D.,
Distinguished Professor of Law
Amy Bitterman, B.A., J.D.,
Assistant Clinical Professor of Law
Elise Boddie, B.A., M.P.P., J.D.,
Professor of Law
Linda S. Bosniak, A.B., M.A., J.D., Ph.D.,
Distinguished Professor of Law
Esther Canty-Barnes, B.A., J.D.,
Clinical Professor of Law
Michael A. Carrier, B.A., J.D.,
Board of Governors Professor
Victoria Chase, B.A., J.D.,
Associate Dean for Academic Affairs and Associate Clinical Professor of Law
Ronald K. Chen, A.B., J.D.,
University Professor and Distinguished Professor of Law
Todd Clear, B.A., M.A., Ph.D.,
University Professor
Laura Cohen, B.A., J.D.,
Distinguished Clinical Professor of Law
Jean-Marc Coicaud, Doctorat D'Etat, Ph.D.,
Distinguished Professor of Law
Jorge Contesse, LL.B., LL.M.,
Associate Professor of Law
Rose Cuison-Villazor, B.A., J.D., LL.M,
Professor of Law and Chancellor's Social Justice Scholar

Sarah Dadush, B.A., J.D., LL.M.,
Professor of Law
Perry Dane, B.A., J.D.,
Professor of Law
Kelly Deere, J.D.,
Assistant Clinical Professor of Law
Donna I. Dennis, B.A., M.A., J.D., Ph.D.,
Professor of Law
Jon C. Dubin, A.B., J.D.,
Associate Dean for Clinical Education and Board of Governors Distinguished Public Service Professor of Law
Douglas S. Eakeley, B.A., A.B. (Oxon.), M.A., J.D.,
Alan V. Lowenstein Professor of Corporate and Business Law and Distinguished Professor of Professional Practice
Katie Eyer, B.A., J.D.,
Professor of Law
Jay M. Feinman, B.A., J.D.,
Distinguished Professor of Law
Gary L. Francione, B.A., M.A., J.D.,
Board of Governors Professor and Distinguished Professor of Law
David M. Frankford, B.A., J.D.,
Professor of Law
Ann E. Freedman, B.A., J.D.,
Associate Professor of Law
Sandy Freund, B.A., J.D., LL.M.,
Clinical Professor of Law
Steven F. Friedell, B.A., J.D.,
Professor of Law
Matteo Gatti, J.D., LL.M., S.J.D.,
Professor of Law
Rachel Godsil, B.A., J.D.,
Distinguished Professor of Law
Steve C. Gold, A.B., J.D.,
Professor of Law
Sally F. Goldfarb, B.A., J.D.,
Professor of Law
Carlos González, B.A., M.A., J.D.,
Professor of Law
Ellen P. Goodman, A.B., J.D.,
Associate Dean of Strategic Initiatives and Special Projects, Professor of Law
Joanne Gottesman, B.A., J.D.,
Clinical Professor of Law
Barbara Gotthelf, B.A., J.D.,
Professor of Professional Practice of Law
Stuart P. Green, B.A., J.D.,
Distinguished Professor of Law
Anjum Gupta, B.A., J.D.,
Professor of Law
Yuliya Guseva, LL.B., M.A., S.J.D., LL.M., *Professor of Law*
Phoebe Haddon, B.A., J.D., LL.M.,
Professor of Law
Adil A. Haque, A.B., J.D.,
Professor of Law
Philip L. Harvey, B.A., J.D., Ph.D.,
Professor of Law
Stacy Hawkins, B.A., J.D.,
Vice Dean and Professor of Law
Norrinda Hayat, B.A., J.D.,
Associate Clinical Professor of Law and Director of the Civil Justice Clinic
Taja-Nia Y. Henderson, A.B., M.A., J.D., Ph.D.,
Professor of Law
Christina S. Ho, A.B., M.P.P., J.D.,
Professor of Law
Barbara Hoffman, A.B., J.D.,
Clinical Associate Professor of Law
Robert Holmes, B.A., J.D.,
Distinguished Clinical Professor of Law
Alan S. Hyde, A.B., J.D.,
Distinguished Professor of Law
Richard Hyland, A.B., M.F.A., J.D., D.E.A.,
Distinguished Professor of Law
Pam Jenoff, B.A., M.A., J.D.,
Clinical Professor of Law
John Joergensen, B.A., M.S., M.A.L.S., J.D.,
Professor of Law
Thea Johnson, A.B., J.D.,
Associate Professor of Law
Margo Kaplan, B.S., M.P.A., J.D.,
Professor of Law
Alexis Karteron, B.A., J.D.,
Clinical Professor of Law
John R. Kettle, III, B.A., J.D.,
Clinical Professor of Law
Suzanne A. Kim, B.A., J.D.,
Associate Dean of Academic Research Centers, Professor of Law
Emily Kline, B.A., J.D.,
Assistant Clinical Professor of Law
Donald Korobkin, B.A., A.M., J.D.,
Professor of Law
Kathryn E. Kovacs, B.A., J.D.,
Professor of Law
Arthur B. Laby, B.A., J.D.,
Vice Dean, Professor of Law
John Leubsdorf, B.A., M.A., J.D.,
Distinguished Professor of Law
Michael A. Livingston, A.B., J.D.,
Professor of Law
David Lopez, B.A., J.D.,
Professor of Law, Prof. Alfred Slocum Scholar
John C. Lore, III, B.A., J.D.,
Distinguished Clinical Professor of Law
Earl M. Maltz, B.A., J.D.,
Distinguished Professor of Law
Randi Mandelbaum, B.S., J.D., LL.M.,
Distinguished Clinical Professor of Law
Kimberly Mutcherson, B.A., J.D.,
Professor of Law
Alison M. Nissen, B.A., J.D.,
Clinical Associate Professor of Law

David L. Noll, B.A., J.D.,
Associate Dean for Faculty Research and Development, Professor of Law
John F. K. Oberdiek, B.A., M.A., J.D., Ph.D.,
Distinguished Professor of Law
Chrystin Ondersma, B.A., J.D.,
Professor of Law
Brandon Paradise, B.A., J.D.,
Associate Professor of Law
Dennis M. Patterson, B.A., M.A., J.D., Ph.D.,
Board of Governors Professor and Distinguished Professor of Law
Twilla Perry, B.A., M.S.W., J.D.,
Professor of Law
Louis S. Raveson, B.A., J.D.,
Professor of Law
Harry M. Rhea, B.A., M.S., M.A., Ph.D.,
Associate Professor of Criminal Justice and Law
Sarah Ricks, B.A., J.D.,
Distinguished Clinical Professor of Law
Ruth Anne Robbins, B.A., J.D.,
Distinguished Clinical Professor of Law
Andrew Rossner, B.A., M.A., J.D.,
Associate Dean for Professional & Skills Education and Distinguished Professor of Law
Andrew J. Rothman, B.A., M.F.A., J.D.,
Professor of Professional Practice and Managing Attorney of Rutgers Law Associates
Jacob Hale Russell, B.A., M.A., J.D.,
Associate Professor of Law
Sabrina Safrin, B.A., J.D.,
Professor of Law
Adam Scales, B.A., J.D.,
Professor of Law
Meredith Schalick, B.A., M.S., J.D.,
Clinical Professor of Law
Fadi Shaheen, LL.B., LL.M., S.J.D.,
Professor of Law
Matthew Shapiro, A.B., D.PHIL., J.D.,
Associate Professor of Law
Sandra Simkins, B.A., J.D.,
Distinguished Clinical Professor of Law
Amy Soled, B.A., J.D.,
Clinical Associate Professor of Law
Rayman Solomon, B.A., M.A., J.D., Ph.D.,
University Professor
Allan R. Stein, B.A., J.D.,
Professor of Law
Beth Stephens, B.A., J.D.,
Distinguished Professor of Law
Rick Swedloff, B.A., J.D.,
Professor of Law
George C. Thomas III, B.S., M.F.A., J.D., LL.M., S.J.D., *Board of Governors Professor and Distinguished Professor of Law*
David Dante Troutt, A.B., J.D.,
Distinguished Professor of Law
Jennifer Rosen Valverde, B.A., M.S.W., J.D.,
Distinguished Clinical Professor of Law
Penny Venetis, B.A., M.A., J.D.,
Distinguished Clinical Professor of Law
Jacob Victor, A.B., J.D.,
Assistant Professor of Law
Alec Wallen, B.A. J.D., Ph.D.,
Professor of Law
Carol Wallinger, B.S., J.D.,
Clinical Professor of Law
Mark S. Weiner, A.B., J.D., Ph.D.,
Professor of Law
Reid K. Weisbord, B.S., J.D.,
Professor of Law
Amy Widman, B.A., J.D.,
Clinical Associate Professor of Law
Adnan Zulfiqar, B.A., M.A., M.L.S., J.D., *Associate Professor of Law*

Law Library Faculty

Marjore E. Crawford, B.A., M.L.I.S.
Wei Fang, B.S., M.L.I.S., M.S.C.S.
Dennis Kim-Prieto,
B.A., M.S.L.I.S., M.F.A., J.D.
Rebecca Kunkel, B.A., J.D., M.L.I.S.
Jootaek Lee, M.A., J.D., M.L.S.
Heather Mitchell, B.A., M.A., M.L.I.S.
Charlotte D. Schneider, B.B.A., J.D., M.B.A.,M.S.L.I.S.
Judith Simms, B.A., J.D.
Nancy B. Talley, B.A., J.D., M.S.
Caroline Young, B.A., M.S.L.I.S., J.D.
Jingwei Zhang, LL.B, LL.M

Adjunct Faculty

Bruce Afran
Abed Awad
Megan Bannigan
Richard Barkasy
Christine V. Bator
Maureen Behm
Brian Berkley
Jonathan D. Bick
Pablo N. Blanco
Jay Blumberg
Paul Bond
Andrew Bondarowicz
Hal Braff
Susan Bricklin
Sheldon Bross

John M. Cannel
Carolyn Campanella
Robert D. Chesler
Hon. James B. Clark III
Roger W. Clark
Arnold S. Cohen
Robert Cooper
Marc Davies
Megan Davies
Derek Decosmo
Raquel Destephano
Michael R. Dichiara
Hon. Ann Donio
Linda Effenbein
Brenda Eutsler
Barry Evenchick
Hon. Mark Falk
Veronica Finkelstein
Brian Foley
Hon. Travis L. Francis
David Frizell
Angie Gambone
Kevin Gardner
Daniel Garrie
J. Patrick Geraghty
Robert S. Goldsmith
Bruce I. Goldstein
Faith Greenfield
Debra E. Guston
Janet Hallahan
Ryan A. Hancock
Hon. Dorothy Harbeck
Hon. Noel Hillman
Herb Hinkle
Raquiba Huq
Nancy Iannone
Cynthia Jacob
Marc Joaquin
John Kearney
Alex Kemeny
George Kenny
Barry Kitain
Travis Laster
Ronald J. Levine
Michael Macko
Robert J. Macpherson
Ann Mallgrave
Ira B. Marcus
Robert E. Margulies
Bruce Matez
John Mcmahon
William Mcnichol
Angella Middleton
Sheryl Mintz Goski
T. Gary Mitchell
Louis Moffa
Eric Moran
Alison Morris
Hon. Edward M. Neafsey
Brian Neary
Philip Neuer
Mitchel M. Novitzky
Lawrence Orloff
Gwen Orlowski
Michael Parker
Cymie Payne
Tara Pellicori
Caroline Petrilla
Todd Poland
Robert S. Popescu J
Onathan I. Rabinowitz
Hon. David Ragonese
Hon. Eduardo Robreno
Bruce Rosen
Herb Sablove
Hon. Joel Schneider
Matthew Schorr
William Schroeder
Alexander Shalom
Gerald Shanker
Linda Shashoua
Victoria Shilton
Hon. Patty Shwartz
Bill Slover
Heather Stapleton
Hon. Gary Stein
Heidi A. Tallentire
Dennis Talty
Janesa Urbano
Marcus Washington
Richard West
Tim West
Neil Wise
Elspeth Abel
Elizabeth Acevado
Angelica Aguirre
Lisa Alston
Rebecca Baehr
Jeffrey Balog
Joann Brea
Patricia Brown
Loretta Burr
Angela Campione
Virginia Caputo
Mayra Caraballo
Deborah Carr
Bernadette Carter
Roselene Correia
Gina Davila
Clifford Dawkins
Frannie Desimone
Timothy Divito
Christine Dougherty
Rhasheda Douglas
Grace Duffin
Susan Feathers
Andrew Finn
Jill Friedman
Sondra Furcajg
Linda Garbaccio
Roberta Geddis
Tai Gedeon
Elaine Giordano
Arbana Gjoca
Katrina Hall
Jason Hernandez
Denise Higgins
David Horan
Cassandra Hunter
Yvena Hypolite
Wanda James
Habibah Johnson
Denise Johnson-steinert
Melissa Jordan
Deborah Leak
Arlene Lentini
Cassandra Lester-key
Margaret Mccarthy
Pam Mertsock-wolfe
Elizabeth Moore
Josephine Nagle
Nathaniel Nakao
Edgar Otieno
Lenore Pearson
Marie Peeke
Mildred Perez
Christopher Phillips
Sarah K. Regina
Nancy Rubert
Thomas Ryan
Daniel Sanders

Staff and Administration

Carol Shaner
Christopher Slater
Stan Sniecikowski
Donna Tagliaferro
Martha Taylor
Wendi L. Taylor
Amy Timko
Robin Todd
Gwen Tolbert
Cheryl Turk
Marvin Velasco
Rebecca Verona
Elizabeth Yeager
Anita Walton
Claire White
Neil Wise

RUTGERS
JOURNAL OF LAW & PUBLIC POLICY

VOLUME 21 FALL 2023 ISSUE 1

CURRENT ISSUES IN PUBLIC POLICY

ISSN 1934-3736

DEFEND OUR DATA: A CALL ON LAWMAKERS TO STRENGTHEN REPRODUCTIVE HEALTHCARE DATA PRIVACY AFTER THE FALL OF *ROE*

Kristen Bentz

INTRODUCTION

A seventeen-year-old Nebraska girl and her mother were criminally charged under several Nebraska laws after authorities discovered the girl had performed a self-managed abortion in violation of the state's statutory cut-off of 20 weeks' gestation.[1] Law enforcement alleged that the girl had a "miscarriage" at 23 weeks' gestation as a result of ingesting "abortion pills" that her mother acquired, and that each of them later participated in burying fetal remains.[2] At the center of the criminal complaint were electronic messages exchanged between the teenager and her mother on Facebook, the social media platform owned by Meta, which purportedly showed the two discussing plans to obtain abortion medication.[3] Meta provided copies of the messages to law enforcement after a search warrant was served on the company for the information.[4]

When Nebraska officials were investigating this case in or around April 2022, federal constitutional law prohibited states from enacting laws or regulations that unduly burdened or restricted access to abortion care.[5] Presumably, Nebraska's law restricting abortion after 20 weeks' gestation would have likely survived a constitutional challenge if raised back then.[6] Thus, the actions of the mother and her teenage daughter in this case very well could have resulted in criminal charges, even while *Roe* was the law of the land.[7] Since then, however, the Supreme Court concluded that the federal constitutional right to an abortion is no more.[8] Now dozens of states are passing laws that are extraordinarily strict—banning and criminalizing self-

---

[1] Kevin Collier & Minyvonne Burke, *Facebook Turned over Chat Messages between Mother and Daughter Now Charged over Abortion*, NBC NEWS (Aug. 10, 2022, 8:42 AM), https://www.cnbc.com/2022/08/09/facebook-turned-over-chat-messages-between-mother-and-daughter-now-charged-over-abortion.html; *See also* NEB. REV. STAT. ANN. § 28-3106 (LexisNexis 2023) (prohibiting the performance of an abortion 20 or more weeks postfertilization with few exceptions).

[2] Collier & Burke, *supra* note 1.

[3] Collier & Burke, *supra* note 1.

[4] Collier & Burke, *supra* note 1.

[5] Roe v. Wade, 410 U.S. 113 (1973); Planned Parenthood v. Casey, 505 U.S. 833 (1992); Stenberg v. Carhart, 530 U.S. 914 (2000); Whole Woman's Health v. Hellerstedt, 579 U.S. 582 (2016).

[6] *Roe*, 410 U.S. at 113; *Casey*, 505 U.S. at 833; *Whole Woman's Health*, 579 U.S. at 582.

[7] Andrea Rowan, *Prosecuting Women for Self-Inducing Abortion: Counterproductive and Lacking Compassion,* GUTTMACHER INST. (Sept. 22, 2015), https://www.guttmacher.org/gpr/2015/09/prosecuting-women-self-inducing-abortion-counterproductive-and-lacking-compassion.

[8] *See* Dobbs v. Jackson Women's Health Organization, 142 S. Ct. 2228, 2242 (2022) ("We hold that *Roe* and *Casey* must be overruled. The Constitution makes no reference to abortion, and no such right is implicitly protected by any constitutional provision, including the one on which the defenders of *Roe* and *Casey* now chiefly rely—the Due Process Clause of the Fourteenth Amendment.").

managed abortion in some instances—thus casting a wide net over individual reproductive healthcare decisions that could become the subject of intense criminal investigation.[9] This remarkable change in constitutional law and the subsequent response of states swiftly passing harsher laws necessitates a review of what exactly is at stake in terms of preserving one's privacy in making reproductive healthcare decisions, and sharing their personal information on the internet.[10] The Nebraska case offers one clear indication: web-based user data may be a powerful tool for law enforcement in states where abortion is illegal, particularly when research shows that internet searches related to abortion are higher in those states.[11]

State officials and prosecutors in states where abortion is illegal are not the sole beneficiaries of abortion-related user data[12], however. It is commonly understood that law enforcement must abide by strict procedural requirements in order to obtain information from third parties during investigations, including things like obtaining a search warrant, issuing a subpoena, or securing a court order.[13] But, non-governmental entities are not so bound. Consider the following hypothetical: a pregnant person residing in a state where abortion is illegal is considering abortion and wants to research their options. That person types "abortion near me" into an internet search engine on their smartphone device and accesses a website advertising

---

[9] Laura Huss, Farah Diaz-Tello & Goleen Samari, *Self-Care, Criminalized: The Criminalization of Self-Managed Abortion From 2000 to 2020,* IF/WHEN/HOW: LAWYERING FOR REPRODUCTIVE JUSTICE, at 61 (2023) (suggesting that prosecutions of self-managed abortion will increase as states pass new laws criminalizing the treatment).

[10] *See After Roe Fell: Abortion Laws by State*, CTR. FOR REPROD. RTS., https://reproductiverights.org/maps/abortion-laws-by-state/ (last visited May 14, 2024) (nationwide survey of abortion laws by state).

[11] Of note, a 2020 study found that states with policies restricting or blocking access to abortion or contraceptive care had significantly higher rates of internet searches using Google for terms like "abortion" or "abortion pills." *See* Sylvia Guendelman et al., *Shining the Light on Abortion: Drivers of Online Abortion Searches across the United States in 2018*, PLOS ONE (May 21, 2020), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0231672. The study also suggested that state laws restricting or banning abortion had little impact on the rates of abortion, as the data showed individuals in those states were not deterred from seeking information about medication abortion online. *Id.* The significance here is that, in the absence of brick-and-mortar abortion clinics offering in-person abortion services, those seeking such contraceptive services turn to the Internet for guidance. *Id.*

[12] Adam Schwartz, *Sen. Wyden Exposes Data Brokers Selling Location Data to Anti-Abortion Groups That Target Abortion Seekers,* ELEC. FRONTIER FOUND. (Feb. 27, 2024), https://www.eff.org/deeplinks/2024/02/sen-wyden-exposes-data-brokers-selling-location-data-anti-abortion-groups-target.

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

abortion counseling in a neighboring state where abortion is legal. That person schedules an appointment on the website, inputting their name, phone number, and email address, all the while believing the website belonged to a *bona fide* abortion clinic. Instead, the website belongs to a pro-life resource center that does not perform abortions or provide licensed medical care.[14] That center now possesses the pregnant person's contact information and, if the website utilizes cookies,[15] may possess other unique information such as the person's IP address,[16] certain web browser data and cross-site activity as well. Consequently, that person is powerless to dictate whether or how the center uses their personal information, including whether it is used to send unsolicited communications intending to dissuade abortion, or shared with other affiliate groups with similar anti-abortion policy goals.[17] It is also not a stretch to suggest that such groups could send the information to law enforcement agencies and alert them of their belief that a pregnant person is pursuing an unlawful abortion.

Internet activity of the type described above occurs hundreds of thousands of times each day in the United States. In 2018, 56% of American adults reported managing their health using websites, 46% using mobile phones/tablets, 35% using social media, and 33% using wearable technology.[18] In a separate study, 35% of American adults reported searching online for information about a medical condition, with women reportedly

---

[14] Pro-life organizations are known to operate "crisis pregnancy centers" that host websites, often with ambiguous references to abortion, that are purposely designed to obfuscate their anti-abortion policies to deceive users into believing the centers provide comprehensive pre-natal healthcare, inducing users to visit their offices seeking a full range of medical options only to be intensely counseled against abortion. *See* Jenifer McKenna & Tara Murtha, *Designed to Deceive: A Study of the Crisis Pregnancy Center Industry in Nine States,* ALL.: STATE ADVOCS. FOR WOMEN'S RTS. & GENDER EQUAL. 5, 6, 10, 35-36, https://www.womenslawproject.org/wp-content/uploads/2022/02/Alliance_CPC_Report_FINAL2-1-22.pdf (last visited May 14, 2024).

[15] "Cookies" are small files that websites deposit on a user's computer that allow the website to track when the user visits the site and how the user interacts with the site. *See* David Nield, *Here's All the Data Collected from You as You Browse the Web,* GIZMODO (Dec. 6, 2017), https://gizmodo.com/heres-all-the-data-collected-from-you-as-you-browse-the-1820779304.

[16] A user's IP (Internet Protocol) address reveals a user's approximate geographic location, as well as the name of a user's internet service provider. *IP Address*, SSD.EFF.ORG, https://ssd.eff.org/glossary/ip-address (last visited May 14, 2024).

[17] Abigail Abrams, *Exclusive: Elizabeth Warren and Senate Democrats Press Crisis Pregnancy Centers on Abortion Data Gathering*, TIME (Sept. 21, 2022, 1:13 PM), https://time.com/6214503/elizabeth-warren-crisis-pregnancy-centers-abortion-data/.

[18] *2018 Consumer Survey on Digital Health*, ACCENTURE, https://www.accenture.com/t20180306T103559Z__w__/us-en/_acnmedia/PDF-71/accenture-health-2018-consumer-survey-digital-health.pdf (last visited May 14, 2024).

conducting searches more than men.[19] Of that same group, 77% reported starting their searches with Google, Bing, or Yahoo search engines.[20] Consider the results of that study with some figures about online activity related to abortion. In 2015, approximately 3.4 million Google searches were conducted for abortion clinics, while more than 700,000 Google searches were conducted with terms related to self-induced abortion.[21] And in the week following the leak of the draft *Dobbs* opinion, medication abortion was searched 350,000 times on Google, representing a 162% increase from the typical search volume for medication abortion.[22]

As the data suggests, a majority of Americans spend a great deal of time searching for medical information online, creating a digital trail with an abundance of personal information. In the United States, there is no comprehensive federal data privacy law that encompasses all categories of data across all industries, which purports to regulate how private entities can collect, store, share, sell, or otherwise use the digital information that users generate.[23] Private corporations and website operators largely have sole discretion whether or not to employ a privacy policy, provided those companies comply with the data privacy requirements of the few states that have passed laws governing data collection.[24]

The public sector also benefits from the massive trove of user data available. Law enforcement agencies employ controversial methods to obtain personal user data, such as purchasing user location data aggregated by data companies for advertising purposes, entirely outside of the judicial process.[25] Thus, with the increase in abortion bans, prosecutors will no doubt direct their investigatory efforts towards obtaining the digital data of the accused from data brokers, web-based enterprises, web-capable devices, mobile app and software developers, and internet service providers ("ISPs"), each of which

---

[19] *Health Online 2013,* PEW RES. CTR. 2 (Jan. 15, 2013), https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/PIP_HealthOnline.pdf.
[20] *Id.* at 3.
[21] Seth Stephens-Davidowitz, *The Return of the D.I.Y. Abortion,* N.Y. TIMES (Mar. 5, 2016), https://www.nytimes.com/2016/03/06/opinion/sunday/the-return-of-the-diy-abortion.html?mcubz=0&_r=0.
[22] Adam Poliak et al., *Internet Searches for Abortion Medications Following the Leaked Supreme Court of the United States Draft Ruling*, JAMA NETWORK 1003 (June 29, 2022), https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2793813 (click "Download PDF" to access the article).
[23] *See Enforcement of Privacy Laws*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/data-protection/enforcement-of-privacy-laws/ (last visited May 14, 2024).
[24] As of this writing, only California, Virginia, Connecticut, Colorado, Utah, Iowa, Indiana, Tennessee, Oregon, Texas, and Montana have passed comprehensive data privacy legislation, while over a dozen others have proposed laws with similar protections. *See Which States Have Consumer Data Privacy Laws?*, BLOOMBERG L. (Sept. 7, 2023), https://pro.bloomberglaw.com/brief/state-privacy-legislation-tracker/.
[25] *See* discussion *infra* Part III, and n. 216.

continuously, and often surreptitiously, collects, stores and shares information about user activity.[26]

This note will proceed in three parts, in which I will analyze the ways that prosecutors, litigants, anti-abortion organizations and tech industry giants contribute to and benefit from virtually unrestricted access to Americans' personal lives by availing themselves of the troves of consumer data that is endlessly collected, stored, shared, sold and transferred. This note will discuss ways these and other groups can and will rely on this data to pursue prosecutions, target individuals with civil litigation, and threaten to diminish access to safe and available abortion and reproductive healthcare treatments in the United States.

Part I will begin with the Supreme Court's *Dobbs* decision and its impact on abortion in the U.S. The discussion will survey the current state laws on abortion and highlight several states' efforts to both ban abortion and pass complicated legislation creating civil private rights of action against healthcare providers and others accused of aiding and abetting abortions. It will introduce some of the policy positions that big tech companies adopted in light of the *Dobbs* opinion related to their data and privacy practices.

Part II will identify some pre-existing federal laws that purport to offer some privacy protection, although not comprehensive enough to account for the recent shift in abortion law. It will examine some of the latest federal and state legislative proposals seeking to bolster data privacy in response to *Dobbs*. Finally, it will analyze proposed regulatory actions of federal agencies in response to a series of executive orders signed by President Joe Biden seeking to address reproductive healthcare data privacy after *Dobbs*.

Lastly, Part III will evaluate whether the Fourth Amendment's protection from unreasonable search and seizure ought to extend to information a user freely gives to third-parties, like wireless carriers and websites. This will include a discussion of a recent legislative proposal to codify the Fourth Amendment's protections from warrantless search and seizure. It will also consider Fourth Amendment jurisprudence as it relates to a mobile app user's reasonable expectation of privacy under the third-party doctrine, particularly with respect to critically important location data that is often obtained via a commonly used data collection technique, geofencing.

---

[26] *See* Kade Crockford & Nathan Freed Wessler, *Impending Threat of Abortion Criminalization Brings New Urgency to the Fight for Digital Privacy,* ACLU (May 17, 2022), https://www.aclu.org/news/privacy-technology/impending-threat-of-abortion-criminalization-brings-new-urgency-to-the-fight-for-digital-privacy.

I. THE FALL OF *ROE* AND THE NATION'S RESPONSE

In June 2022, the Supreme Court issued its opinion in *Dobbs v. Jackson Women's Health Center*, holding that the United States Constitution does not grant the right to an abortion.[27] Animating the Court's decision was the majority's view that abortion rights are neither expressly stated in the Constitution, nor embedded in the history and traditions adhered to in this country.[28] As a result, the Court overruled nearly fifty years of precedent, abrogating the abortion rights that were previously established through the Due Process Clause of the Fourteenth Amendment.[29] The issue of abortion was thus returned to the states, where elected lawmakers have wasted no time passing laws and implementing strict regulations governing abortion without concern of fulfilling a federal constitutional right.[30]

A. Abortion returned to the states

Nearly two years after the Court issued its opinion in *Dobbs*, abortion is now illegal in fourteen states, with only some of those states authorizing the procedure in limited medical emergencies.[31] Yet, even in cases of emergency, medical professionals practicing in those states are hesitant to provide abortions for fear of violating the law.[32] Provider hesitancy is not surprising, since some of the country's most stringent abortion laws threaten severe penalties, including loss of medical license, thousands of dollars in fines, and sentences of life in prison.[33] For the most part, states outlawing abortion have

---

[27] Dobbs v. Jackson Women's Health Ctr., 142 S. Ct. 2228, 2242 (2022).
[28] *Id.* at 2242-43.
[29] *Id.* at 2248 ("Instead, guided by the history and tradition that map the essential components of our Nation's concept of ordered liberty, we must ask what the Fourteenth Amendment means by the term 'liberty.' When we engage in that inquiry in the present case, the clear answer is that the Fourteenth Amendment does not protect the right to an abortion.").
[30] *Tracking Abortion Bans Across the Country,* NYTIMES (last updated Jan. 8, 2024, 9:30 A.M.), https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html.
[31] *Interactive Map: US Abortion Policies and Access After Roe*, GUTTMACHER INST., https://states.guttmacher.org/policies/ (last visited May 14, 2024) (including Idaho, North Dakota, South Dakota, Indiana, Missouri, Arkansas, Oklahoma, Texas, Louisiana, Mississippi, Alabama, Tennessee, Kentucky, and West Virginia as states banning abortion).
[32] *See, e.g.,* Center for Reproductive Rights, *Zurawski v. State of Texas,* CTR. FOR REPROD. RTS. (Mar. 6, 2023), https://reproductiverights.org/case/zurawski-v-texas-abortion-emergency-exceptions/zurawski-v-texas/ (lawsuit alleging ambiguity as to the definition of "medical emergenc[ies]" exception in Texas' abortion statute).
[33] Eleanor Klibanoff, *Texans Who Perform Abortion Now Face up to Life in Prison, $100,000 Fine*, TEX. TRIB. (Aug. 25, 2022, 5:00 AM), https://www.texastribune.org/2022/08/25/texas-trigger-law-abortion/; TEX. HEALTH & SAFETY CODE §§ 170A.001–7; *see also* H.B. 1280 87th Leg., (Tex. 2021) (authorizing a total abortion ban to take effect thirty days after "the

generally not imposed penalties on individuals seeking the abortion; rather, penalties have tended to attach to the procedure itself, thus limiting liability to abortion providers.[34] However, emboldened by the *Dobbs* decision, ideological groups are now pushing more aggressively for "abortion abolition" in their fight for a national abortion ban, and are calling for state legislation that imposes criminal penalties on individuals obtaining abortions.[35]

Some lawmakers are heeding the abolitionists' calls. For example, an Oklahoma state senator proposed a legislative amendment to eliminate a statutory provision that expressly prohibited criminal charges against a woman for the death of her unborn child as a result of an abortion.[36] South Carolina lawmakers went even further with a proposed bill that would designate abortion the same as homicide, rendering the death penalty available for anyone that obtains an abortion.[37] In Arkansas, representatives introduced a bill that would protect "innocent human life" from "the time of fertilization," and specifically grant "unborn children" the right to "be protected under the state homicide laws."[38] Even prior to *Dobbs*, a state representative in Louisiana introduced a bill that, in its original form, would have expanded the definitions of "person" and "unborn child" to encompass fertilization in order for the state's pre-existing criminal laws on homicide to apply to abortions.[39]

Much of this legislation at least implicitly embraces the pro-life belief that life begins at conception, and all "unborn children" are therefore entitled to the same legal rights that living humans enjoy.[40] The Alabama Supreme Court added legitimacy to this belief when it recently decided that frozen embryos designated for in vitro fertilization fall within the legal definition of

---

issuance of a United States Supreme Court judgment in a decision overruling . . . Roe v. Wade . . . .").

[34] Shefali Luthra, *Abortion Bans Don't Prosecute Pregnant People. That May Be about to Change.,* THE 19TH (Jan. 13, 2023, 1:05 PM), https://19thnews.org/2023/01/abortion-bans-pregnant-people-prosecution/.

[35] Rose Conlon, *Abortion Rights Opponents Across the Country Want to Charge Women with Murder,* NPR (July 13, 2023, 5:06 AM), https://www.npr.org/2023/07/13/1187435403/abortion-abolitionists-across-the-country-want-to-charge-women-with-murder.

[36] S.B. 287, 59th Gen. Assemb., Reg. Sess. (Okla. 2023); *See* Press Release, Sen. Warren Hamilton, Hamilton's Bills Assigned to Senate Committees (Feb. 3, 2023), https://oksenate.gov/press-releases/hamiltons-bills-assigned-senate-committees?back=/senator-press-releases/warren-hamilton%3Fpage%3D0.

[37] H.B. 3549, 125th Gen. Assemb., Reg. Sess. (S.C. 2023).

[38] H.B. 1174, 2023 Leg., Reg. Sess. (Ark. 2023).

[39] H.B. 813, 2022 Leg., Reg. Sess. (La. 2022); See also Jessica Kutz, *Pushback on Louisiana's Scuttled Abortion Bill Reveals a Limit on How Far Anti-abortion Groups Are Willing to Go*, THE 19TH (May 13, 2022, 1:11 PM), https://19thnews.org/2022/05/louisiana-law-anti-abortion-group-limits/.

[40] Kate Zernike, *Is a Fetus a Person? An Anti-Abortion Strategy Says Yes.,* N.Y. TIMES (June 21, 2023), https://www.nytimes.com/2022/08/21/us/abortion-anti-fetus-person.html.

"unborn children" for purposes of the state's wrongful death statute.[41] State lawmakers and anti-abortion advocates will no doubt be motivated by this ruling to continue their efforts in enacting laws aimed at expanding the rights of the "unborn."[42]

Many in the anti-abortion circle subscribe to the fetal personhood theory that life begins at conception, yet enacting laws imposing criminal penalties on the individual obtaining an abortion is still a divisive topic among many pro-life organizations.[43] There is concern among that community that as the fringe abolitionist groups gain a wider audience, more states could begin introducing such bills embracing the theory, thus creating a greater chance that some of those bills might be passed into law.[44] Those concerns are not fictional. As of February 15, 2024, thirty-six legislative proposals to ban all or most abortions have been introduced in state legislatures, with another seven proposals seeking to criminalize individuals receiving an abortion and/or the abortion provider.[45]

Apart from implementing laws that are enforced by state officials, some states have passed laws creating civil private rights of action against anyone performing, or aiding and abetting the performance of, an abortion.[46] In Texas, for example, private citizens can file an action against someone accused of performing abortions, and request penalties of up to $10,000 per suspected abortion.[47] Notably, one lawsuit was filed pursuant to this law charging an abortion provider with allegedly providing an abortion, but the case was dismissed by the trial court judge on the grounds that the plaintiff lacked

---

[41] LePage v. Ctr. For Reprod. Med., P.C., 2024 Ala. LEXIS 60, at *9 (Ala. Feb. 16, 2024).
[42] Celine Castronuovo, *Alabama Embryo Ruling Gives Boost to Fetal Personhood Movement,* BLOOMBERG LAW (Feb. 21, 2024, 1:48 P.M.), https://news.bloomberglaw.com/health-law-and-business/alabama-embryo-ruling-gives-boost-to-fetal-personhood-movement.
[43] Poppy Noor, *Republicans push wave of bills that would bring homicide charges for abortion,* THE GUARDIAN (Mar. 10, 2023), https://www.theguardian.com/us-news/2023/mar/10/republican-wave-state-bills-homicide-charges.
[44] Elizabeth Dias, *After Abortion Ruling, a Push for Punishment*, N.Y. TIMES, July 2, 2022, at A1.
[45] *State Legislation Tracker,* GUTTMACHER INST., https://www.guttmacher.org/state-legislation-tracker (last visited May 14, 2024).
[46] *See* TEX. HEALTH & SAFETY CODE ANN. § 171.208 (2021) (authorizing private civil actions against any person who "performs or induces an abortion," or "knowingly engages in conduct that aids or abets the performance or inducement of an abortion"); OKLA. STAT. TIT. 63, § 1-745.35 (2022) (utilizing the same language as the Texas law); IDAHO CODE § 18-8807 (2022) (authorizing private civil actions maintained by individuals with certain familial relation to "any female upon whom an abortion has been attempted or performed" against medical professionals who "knowingly or recklessly attempted, performed, or induced the abortion").
[47] Alan Feuer, *The Texas Abortion Law Creates a Kind of Bounty Hunter. Here's How It Works.*, N.Y. TIMES (Nov. 1, 2021) https://www.nytimes.com/2021/09/10/us/politics/texas-abortion-law-facts.html.

standing.[48] Oklahoma enacted a copycat version of Texas' 6-week ban and accompanying private right of action provision; however, those laws were deemed unconstitutional.[49]

Citizens are also pursuing novel legal theories by lodging pre-existing state law claims against individuals accused of aiding and abetting abortions. A Texas man, for example, filed a wrongful death lawsuit against three women, contending they assisted his ex-wife with obtaining medication to induce an abortion.[50] The legal theory advanced in this suit—applying state tort law to pursue damages for an abortion that the plaintiff claims constitutes murder under Texas law—is perhaps the first of its kind.[51] In the complaint, the plaintiff referenced text messages he obtained from his wife's cell phone, showing the women discussing ways to obtain medication abortion on the internet.[52] This case serves as a preview of what could become the new normal: prosecutors and civil litigants relying on digital data, like internet searches and text messages, to support claims for violations of state laws prohibiting abortion; a suggestion that is all the more plausible considering research indicates that internet search activity related to abortion continues to increase regardless of the severity of the state laws restricting or banning abortion.[53]

Perhaps in recognition of the reported increase in online activity related to abortion[54], some states are also exploring ways to monitor and control the digital flow of information about abortion. For example, an Iowa lawmaker introduced a bill that would allow the state to track Iowans' online activity, specifically any online research conducted concerning abortion.[55] To achieve this, the state would establish a computer database, controlled and maintained by the Iowa Department of Human Services.[56] The Department would vet contracts with "pregnancy resource centers" that would collect data from Iowans in real-time through the use of targeted digital marketing tools

---

[48] Eleanor Klibanoff, *Texas State Court Throws out Lawsuit Against Doctor Who Violated Abortion Law,* TEX. TRIB. (Dec. 8, 2022, 2:10 PM), https://www.texastribune.org/2022/12/08/texas-abortion-provider-lawsuit/.

[49] OKLA. STAT. TIT. 63, § 1-745.31; S.B. 1503, 58th Leg., 2nd Reg. Sess. (Ok. 2022) (6-week, private right of enforcement ban); H.B. 4327, 58th Leg., 2nd Reg. Sess. (Ok. 2022) (total, private right of enforcement ban); Okla. Call v. State, 531 P.3d 117, 122 (Okla. May 2023).

[50] Eleanor Klibanoff, *Three Texas Women Are Sued for Wrongful Death After Allegedly Helping Friend Obtain Abortion Medication*, TEX. TRIB. (Mar. 10, 2023, 4:00 PM), https://www.texastribune.org/2023/03/10/texas-abortion-lawsuit/.

[51] *Id.*

[52] *Id.*

[53] GUENDELMAN ET AL., *supra* note 11, at 14.

[54] Poliak, *supra* n. 22.

[55] H.F. 515, 89th Gen. Assemb., Reg. Sess. (Iowa 2021). This proposal pre-dates the *Dobbs* opinion, but it underscores the point that lawmakers have long been thinking about ways to utilize digital data to regulate abortion. *Id.* This bill did not proceed out of committee. *Id.*

[56] *Id.*

that can geolocate individuals actively researching abortion online.[57] The pregnancy resource centers would then proactively connect with those Iowans to try and deter abortion by "creat[ing] a conversation" with them, and "encourag[ing] them to choose an alternative to abortion."[58] This highly sensitive user information would be collected by these private organizations (many of which embrace pro-life religious-based views) under contract with the government to disseminate anti-abortion misinformation.[59]

The aforementioned scheme illustrates efforts by public officials to both pass laws banning and criminalizing abortion, and laws to monitor user data and mine the information of private citizens. However, as the following section discusses, private sector corporations also routinely employ dangerous and invasive data gathering tactics that have significant implications for individuals' right to informational privacy.

B. Scrutiny Over Big Tech's Privacy Policies After Dobbs

Immediately following the issuance of *Dobbs*, public debate erupted over whether, or how, big tech companies could reconcile the mass amounts of data they collect from users given the possibility that such data may be sought out to support abortion-related prosecutions.[60] The developing question was whether, and to what extent, big tech would cooperate with authorities' investigations into abortion-related crimes.[61] Some of this questioning came from investor groups advocating for corporate support for reproductive rights, who voiced concern about whether companies were planning to protect their workforces if abortion were made illegal.[62] Meanwhile, privacy advocates pointed out many companies' troubling data practices. For example, one research group exposed at least 294 websites owned by crisis pregnancy centers utilized Facebook's advertisement

---

[57] *Id.*

[58] *Id.*

[59] Carter Sherman, *Iowa Republican Wants to Track Down Pregnant People with 'Targeted Digital Marketing'*, VICE NEWS (Feb. 19, 2021, 1:29 PM), https://www.vice.com/en/article/n7vyeb/iowa-republican-wants-to-track-down-pregnant-people-with-targeted-digital-marketing-out-of-abortion.

[60] *See* Brian Fung & Clare Duffy, *A Big Question for Tech Companies Post*-Roe*: How to Respond to Law Enforcement Requests for Data?,* CNN (June 28, 2022, 5:03 P.M.), https://www.cnn.com/2022/06/28/tech/big-tech-abortion-data-law-enforcement/index.html; Gerrit De Vynck et. al., *Abortion Is Illegal for Millions. Will Big Tech Help Prosecute It?,* WASH. POST (June 29, 2022, 9:22 P.M.), https://www.washingtonpost.com/technology/2022/06/29/google-facebook-abortion-data/.

[61] De Vynck et al., *supra* note 60.

[62] Jeff Green, *Will Big Tech Protect Abortion Seekers? Investors Want to Know.,* ALM (June 30, 2022, 1:07 PM), https://www.law.com/dailybusinessreview/2022/06/30/will-big-tech-protect-abortion-seekers-investors-want-to-know/?slreturn=20230718095321.

technology code, which allowed the centers to collect and share users' personal data with Facebook.[63] This took place despite Meta's official policy prohibiting any website utilizing their code to share "sexual and reproductive health" data with Facebook.[64] Other researchers discovered that low-income women searching Google for abortion options were disproportionately targeted with advertisements for crisis pregnancy centers, all while Google was earning almost $10 million in ad revenue from these organizations as they paid to optimize their position on search result lists.[65] The researchers created fake Google user accounts that identified as low- or average-income women residing in major American cities like Phoenix and Atlanta, and then conducted searches for information about how to obtain an abortion; the results showed 56% of the searches on the Phoenix-based accounts returned ads for anti-abortion facilities, with nearly 42% on the Atlanta-based accounts.[66]

Unsurprisingly, the public's concern over privacy grew as giants like Amazon, Apple, Lyft, Microsoft, Uber, Snapchat, TikTok and Twitter largely ignored these and other concerns in the wake of the *Dobbs* opinion.[67] When Google eventually announced it would discontinue its practice of storing user location data around abortion clinics, the company was praised.[68] Its announcement came after the Alphabet Workers Union, representing more than 800 people working for Google's parent company Alphabet, demanded that the search engine delete user data that law enforcement could use in abortion cases.[69] Google also emphasized that company policy requires advertisers wanting to appear under search queries related to obtaining an abortion must certify to Google whether they provide abortion services so that

---

[63] Grace Oldham & Dhruv Mehrota, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients,* REVEAL (June 15, 2022), https://revealnews.org/article/facebook-data-abortion-crisis-pregnancy-center/.

[64] *Id.*

[65] Poppy Noor, *Google Targets Low-income US Women with Ads for Anti-abortion Pregnancy Centers, Study Shows,* THE GUARDIAN (Feb. 7, 2023), https://www.theguardian.com/world/2023/feb/07/google-targets-low-income-women-anti-abortion-pregnancy-center-study; *See also,* Kari Paul, *Google Earned $10m from Ads Misdirecting Abortion Seekers to 'Pregnancy Crisis Centers',* THE GUARDIAN (June 23, 2023), https://www.theguardian.com/technology/2023/jun/15/google-misleading-abortion-ads-pregnancy-crisis-centers.

[66] *Google Helps 'Fake Abortion Clinics' Target Low-Income Women,* TECH TRANSPARENCY PROJECT (Feb. 6, 2023), https://www.techtransparencyproject.org/articles/google-helps-fake-abortion-clinics-target-low-income-women.

[67] Fung & Duffy, *supra* note 50.

[68] Nico Grant, *Google Says It'll Delete Location Data When Users Visit Abortion Clinics*, N.Y. TIMES (Jul. 2, 2022), https://www.nytimes.com/2022/07/01/technology/google-abortion-location-data.html.

[69] *Id.*

a disclaimer could appear with the results.[70] Still, some lawmakers probed Google after an investigation showed that the company was not consistently applying search result disclaimers in accordance with its own policy.[71] And in another instance, lawmakers doubted whether Google was following through on its promise to delete location data, after a newspaper investigation revealed that the company was not reliably removing users' recorded visits to Planned Parenthood clinics from its datasets.[72] The latter revelation is not so surprising, especially since Google previously agreed to an almost $400 million privacy settlement with forty states after it was charged with misleading consumers into believing that location tracking settings were turned off while the company continued collecting the information.[73] Nonetheless, Google maintained in responsive remarks that it was committed to removing the location history data for users visiting sensitive locations.[74]

On the whole, Google's public commitment to adjust its data collection practice is a step in the right direction, but it falls woefully short of the necessary actions to address rampant data mining. To cure the public's concerns, Google and other tech companies should consider implementing more proactive measures to execute comprehensive plans that strengthen consumer data privacy.

First, companies should aspire to simply minimize the amount of sensitive data they collect, such that only the data necessary to allow the company to monitor service performance and satisfy consumer needs is collected—and even then, companies should routinely purge user data once it is no longer required to satisfy operational needs. Presumably, companies should already be engaged in data minimization, since retaining data for

---

[70] Paul, *supra* note 65.

[71] Press Release, Sen. Mark Warner, Following New Investigation, Warner & Slotkin Press Google on Misrepresentation in Ads Targeted to Users Searching for Abortion Services (Nov. 22, 2022), https://www.warner.senate.gov/public/index.cfm/2022/11/following-new-investigation-warner-slotkin-press-google-on-misrepresentation-in-ads-targeted-to-users-searching-for-abortion-services.

[72] Brian Fung, *Senate Democrats Write to Google over Concerns about Abortion-seekers' Location Data,* CNN (May 24, 2023, 2:58 PM), https://www.cnn.com/2023/05/24/tech/senate-dems-google-abortion-location-data-concerns/index.html; *See also,* Geoffrey A. Fowler, *Google Promised to Delete Sensitive Data. It Logged My Abortion Clinic Visit.,* WASH. POST (May 9, 2023, 11:23 AM), https://www.washingtonpost.com/technology/2023/05/09/google-privacy-abortion-data/.

[73] Cecilia Kang, *Google Agrees to $392 Million Privacy Settlement with 40 States,* N.Y. TIMES (Nov. 14, 2022), https://www.nytimes.com/2022/11/14/technology/google-privacy-settlement.html?searchResultPosition=1.

[74] Jen Fitzpatrick, *Protecting People's Privacy on Health Topics,* Editor's note to *Original Post*, THE KEYWORD (May 12, 2023), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/.

longer than necessary may violate federal law.[75] And while it is true that, under existing law, data can be disclosed in response to a lawful warrant from law enforcement, from a privacy perspective, the real issue is that the information is available in the first place. Companies should therefore re-evaluate what data is absolutely essential in order to operate their business.

Second, companies that offer messaging features should provide users the ability to send and receive messages using end-to-end encryption.[76] This would offer a level of security to the data that is being transmitted, and would assure users that they can comfortably use the messaging application without fear of their sensitive information being collected. Third, companies must strive to be fully transparent with users about what data is collected, how the data is used, and whether users have the choice to opt-in or opt-out of data collection.[77] This might consist of tracking disclosures on the company's website outlining the types of data that could be released in the event of a request from law enforcement or other regulatory bodies. In addition to being transparent with data collection disclosures, users should be offered the ability to opt-out of data collection—although some data experts suggest the default setting should always be opt-out, so that there would be no doubt that users who choose to opt-in are fully consenting to their data to be collected.[78] This way, users can make informed decisions about what websites they choose to visit and maintain better control of the flow of their information. A default opt-out policy might encourage corporations to offer financial incentives to users to opt-in to data collection, similar to the types of discount incentives that online retailers offer to users that submit to email marketing, for instance.[79] In that case, each party would enjoy some benefit from the exchange of user information.

Facebook's approach provides a useful example of some of the above suggestions. There were immediate and widespread reports in the media after Facebook released information that aided the criminal investigation into the

---

[75] Avi Gesser et. al., *Data Minimization – Recent Enforcement Actions Show Why Some Companies Need to Get Rid of Old Electronic Records,* COMPLIANCE & ENF'T, (May 26, 2022), https://wp.nyu.edu/compliance_enforcement/2022/05/26/data-minimization-recent-enforcement-actions-show-why-some-companies-need-to-get-rid-of-old-electronic-records-2/; *See also* 15 U.S.C. § 45(a)(1).

[76] Ben Lutkevich & Madelyn Bacon, *End-to-End Encryption (E2EE),* TECHTARGET (June 2021), https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE.

[77] *See, e.g.*, Corynne McSherry, *Data Privacy Policy Must Empower Users and Innovation*, EFF (Apr. 4, 2018), https://www.eff.org/deeplinks/2018/04/smarter-privacy-rules-what-look-what-avoid.

[78] Brian Barrett, *Hey, Apple! 'Opt Out' Is Useless. Let People Opt in,* WIRED (Aug. 2, 2019, 4:32 PM), https://www.wired.com/story/hey-apple-opt-out-is-useless/.

[79] Christian Auty, et al., *Colorado's "Loyalty Program" regulations are final and they blow California's rules out of the water,* JD SUPRA (May 30, 2023), https://www.jdsupra.com/legalnews/colorado-s-loyalty-program-regulations-7235418/.

Nebraska teenager accused of self-inducing an abortion.[80] In response, Facebook's parent company Meta issued a statement "[c]orrect[ing] the record," maintaining that the "valid legal warrant[]" served on it by law enforcement did not mention abortion at all, thus dispelling any narrative that Facebook was willingly aiding an abortion prosecution.[81] With respect to the company's handling of legal warrants, Meta's Safety Center provides a transparent explanation of its policy to disclose certain account records in response to such requests:

> A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, timeline posts, and location information.[82]

In another Meta product, Facebook Messenger boasts default end-to-end message encryption, a privacy feature that requires the input of a special numerical key that is unique to the device the messages originate from.[83] The key is required in order for any individual to access or view the conversations.[84] Facebook debuted message encryption in 2016, but users needed to opt-in to the service then, whereas now the service is the default option for all users.[85] According to Facebook, not even Meta is able to access or read the encrypted messages.[86] Federal prosecutors consider encryption settings as "warrant-proof," and refer to companies' decision to permit user encryption as "encourag[ing] more crime," creating a "lawless space where law enforcement is powerless to investigate," and allowing "dangerous

---

[80] *See* Wes Davis, *Meta-provided Facebook Chats Led a Woman to Plead Guilty to Abortion-related Charges,* THE VERGE (Jul. 11, 2023), https://www.theverge.com/2023/7/11/23790923/facebook-meta-woman-daughter-guilty-abortion-nebraska-messenger-encryption-privacy; Shefali Luthra, *Could Facebook Messages Be Used in Abortion-related Prosecution?,* 19TH NEWS (Jul. 20, 2023, 1:11 PM), https://19thnews.org/2023/07/abortion-laws-facebook-messages-digital-privacy/.

[81] Press Release, Meta, Correcting the Record on Meta's Involvement in Nebraska Case (Aug. 9, 2022), https://about.fb.com/news/2022/08/meta-response-nebraska-abortion-case/.

[82] *Information for Law Enforcement Authorities,* META SAFETY CTR., https://about.meta.com/actions/safety/audiences/law/guidelines/ (last visited May 14, 2024)

[83] *End-to-end Encryption,* FACEBOOK, https://www.facebook.com/help/messenger-app/1084673321594605 (last visited May 14, 2024).

[84] *Id.*

[85] Kyle Barr, *Mark Zuckerberg Says They're Finally Rolling Out Default End-to-End Encryption on Messenger,* GIZMODO (Jan. 23, 2023), https://gizmodo.com/facebook-messenger-meta-end-to-end-encryption-1850018975.

[86] *Id.*

criminals to cloak their . . . digital activities behind an impenetrable shield."[87] Nonetheless, at this point Meta's encryption feature is limited, since it is only available to those using Messenger on mobile devices.[88]

Meta's transparency about its information disclosure policy and its end-to-end encryption features are noteworthy of its attempt to offer users some sense of privacy, however the company has been heavily criticized for some significant privacy invasions over the years. It was once discovered that Meta surreptitiously collected and stored a vast amount of user information, including biometric data.[89] A Meta executive also once admitted that selling its user data could be a profitable venture.[90] Somewhat walking those comments back, the company's Chief Privacy Officer more recently claimed that the company does not engage in the practice of *selling* user data.[91] Yet, Meta frequently shares user data. In 2018, a New York Times investigation revealed Meta was sharing user data with several of the largest tech companies in the world at a higher frequency than it had previously claimed.[92] As noted in the Times investigation, Meta had already been embroiled in a prior scandal concerning Facebook user data being shared with Cambridge Analytica, a political organization that used the data to target and influence voters in the run-up to the 2016 United States presidential election, without user knowledge or consent.[93] On this issue, CEO Mark Zuckerberg appeared before

---

[87] *See* Scott Brady, *Scott Brady: Facebook Encryption Could Endanger Victims,* PITTSBURGH POST-GAZETTE (Jan. 10, 2020), https://www.post-gazette.com/opinion/Op-Ed/2020/01/10/Scott-Brady-Facebook-encryption-could-endanger-victims/stories/202001100034; *see* Mike Stuart, *Mike Stuart: Warrant-proof Encryption Threatens Children,* HERALD DISPATCH (Nov. 24, 2019), https://www.herald-dispatch.com/opinion/mike-stuart-warrant-proof-encryption-threatens-children/article_80e89073-059d-5119-b85a-76c7b2278a4f.html; John C. Milhiser, *Guest Commentary | Warrant-proof Encryption Threatens Safety,* NEWS GAZETTE (Dec. 15, 2019), https://www.news-gazette.com/opinion/guest-commentary/guest-commentary-warrant-proof-encryption-threatens-safety/article_ec2c85e3-0b79-5099-a551-8a950d5c6add.html.

[88] Press Release, Melissa Miranda, Expanding Features for End-to-End Encryption on Messenger (Jan. 23, 2023), https://about.fb.com/news/2023/01/expanding-features-for-end-to-end-encryption-on-messenger/.

[89] Malathi Nayak, *Facebook Proposes $650 Million to Settle Biometric Privacy Case*, BLOOMBERG L. (July 23, 2020, 4:55 PM), https://news.bloomberglaw.com/privacy-and-data-security/facebook-proposes-650-million-to-settle-biometric-privacy-case?context=article-related.

[90] Kalev Leetaru, *What Does It Mean For Social Media Platforms to "Sell" Our Data?*, FORBES (Dec. 15, 2018, 3:56 PM), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=52f9a86a2d6c.

[91] Press Release, Michael Protti, Here's What You Need to Know About Our Updated Privacy Policy and Terms of Service (May 26, 2022), https://about.fb.com/news/2022/05/metas-updated-privacy-policy/.

[92] Gabriel J.X. Dance, Michael LaForgia & Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html.

[93] *Id.*

a Congressional joint committee for hours of questioning, offering no meaningful explanation for the company's troubling actions.[94]

For the most part, websites like Google and Facebook collect general user data, like location, cross-site activity, IP address and search history, whereas other companies that specialize in health-related areas collect the same information and then also collect incredibly sensitive personal information.[95] For example, "femtech" refers to products and services offered through apps and websites that focus almost exclusively on women's health needs.[96] As of 2020, over 100 million women downloaded and used menstrual tracking apps.[97] In 2019, femtech was estimated to have generated $820.6 million in global revenue, and by mid-year 2022, femtech reached $3.86 billion in venture capital investment.[98] By 2025, the femtech industry is estimated to be worth almost $50 billion.[99] Popular femtech apps like Flo and Clue track users' ovulation and menstruation.[100] Another app, Ovia, tracks fertility windows and monitors pregnancy progress, and even offers a service product to employers that allows for reviewing aggregated, de-identified[101] health data of employees that use the app, which purportedly offers insight into the number of high-risk pregnancies among their workforce.[102] It's difficult to conceive how employers actually benefit from knowing this information, except perhaps to assist in anticipating health insurance and other employment benefits costs. Regardless, such apps are on the rise in

---

[94] Lucien Bruggeman, *Zuckerberg Faces Congressional Grilling over Facebook User Privacy, 2016 Election*, ABC NEWS (Apr. 11, 2018, 4:15 AM), https://abcnews.go.com/Politics/zuckerberg-faces-congressional-grilling-facebook-user-privacy-2016/story?id=54366595; *see generally Facebook, Social Media Privacy, and the Use and Abuse of Data: Joint Hearing Before the S. Comm. on Commerce, Science and Transportation and the S. Comm. on the Judiciary,* 115th Cong. (2018).

[95] *See generally* Nield, *supra* note 15 (explaining the types of data collected by websites).

[96] Josh Howarth, 20 Impressive FemTech Startups (2023), EXPLODING TOPICS (June 28, 2023), https://explodingtopics.com/blog/femtech-startups.

[97] Leah R. Fowler et. al., Readability and Accessibility of Terms of Service and Privacy Policies for Menstruation-Tracking Smartphone Applications, 21 HEALTH PROMOTION PRAC. 679 (2020).

[98] Howarth, *supra* note 96.

[99] Fowler et. al., *supra* note 97.

[100] *See* Fowler et. al., *supra* note 97.

[101] De-identified generally refers to data that has certain personally identifiable information ("PII") removed, like names, addresses, and dates of birth, while other identifiers like age, gender, or race remain available for research purposes, thus theoretically reducing the likelihood that an individual can be recognized in a group of data. *Data De-identification,* UMASS CHAN MED. SCH., https://www.umassmed.edu/it/security/research-and-clinical-data-access/data-de-identification/.

[102] Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?*, WASH. POST (Apr. 10, 2019, 3:11 PM), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.

popularity, and many have been reviewed by privacy advocate groups looking to identify whether these apps have adequate data privacy policies.[103]

In one study conducted by a non-profit tech company promoting privacy online, 18 out of the 25 reproductive health apps and wearable devices analyzed were assigned a *Privacy Not Included warning label.[104] A majority of the apps analyzed did not have clear guidelines about what data could be disclosed to law enforcement.[105] Shockingly, one app, Sprout Pregnancy, which collects information consisting of doctor appointment dates and birth plans, did not even have a privacy policy.[106] Only one of the reviewed apps, Euki[107], satisfied the researchers' standards, due to the app's practice of storing data locally on users' devices and requiring users to enter two separate passcodes before viewing the contents of the app.[108] The overarching issue is that a great deal of apps have user privacy policies that are tremendously difficult and confusing to read to a lay person, resulting in users being completely unaware what data is being collected.[109]

Because not all companies employ the same privacy standards, largely because there is no uniform data privacy law in the U.S., there is a substantial burden on U.S. consumers to remain vigilant about how they interact online. As discussed, some websites and apps have taken steps towards empowering users with the ability to limit the way their data is used—offering users the ability to opt-out of data collection, for example. But consumers that opt-out of data collection might be punished with an inferior product or diminished services, since most websites that collect data from consumers use that data to improve product performance and curate offers specifically to users based on their behavior or use of the service. Thus, a small incentive exists for users to continue to voluntarily consent to their information being collected. The larger problem, however, is that companies are currently under no uniform legal obligation to affirmatively notify users of what data is being collected, how it is being stored, whether data can be disclosed to law enforcement, or used as a commodity to be sold or transferred to a third party. The path to a solution must begin with robust and comprehensive federal legislation and administrative action.

---

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

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] Euki describes itself as being developed by "privacy experts," and is "designed with privacy in mind." *See* App Store Preview, *Euki,* Apple.com, https://apps.apple.com/us/app/euki/ id1469213846 (last visited May 14, 2024).

[108] *Id.*

[109] *See* Fowler et al., *supra* note 97.

II. A CALL ON LAWMAKERS: PASS LEGISLATION TO STRENGTHEN DATA PRIVACY

As stated, there is no U.S. federal law governing the regulation of web-based user data, and only a small collection of states have data privacy laws governing the ways that user data can be collected, stored, shared, or sold.[110] In addition to the overwhelming public demand that tech companies implement and uphold bold user data privacy initiatives, there is a strong need for the federal government to step up and implement new, comprehensive legislation tackling universal data privacy concerns. An examination of already existing privacy legislation, specifically as related to healthcare, is a necessary first step to inform the most appropriate legislative action to bolster informational privacy. As evinced below, there are a variety of existing laws and regulations that are ripe for modification or amendment to expand individual data privacy.

A. Health Information Portability and Accountability Act

One powerful privacy tool the federal government has at its disposal is the authority to promulgate stronger regulations in the Privacy Rule derived from the Health Insurance Portability and Accountability Act of 1996, commonly referred to as HIPAA, which governs the conditions under which sensitive medical and health information may be disclosed to third parties.[111] It's widely understood that HIPAA guarantees medical information privacy, but few realize just how narrow its protections actually are. In the months following March 2020, when COVID-19 reached the United States, HIPAA was arguably one of the most frequently discussed laws in the news, social media posts and, most prominently, in schools and the workplace.[112] Yet most people's perception of its function was inaccurate.[113] Masking and vaccination requirements, COVID-19 testing rules and similar efforts were initiated by employers, governments, and schools in attempts to curb the spread of the novel coronavirus, but were vehemently resisted by many Americans, including at least one United States Representative, who wrongly assumed

[110] Bloomberg L., *supra* note 24.
[111] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 2713, 110 Stat. 1936 (1996).
[112] Jayme Fraser, et al., *Despite federal guidance, schools cite privacy laws to withhold info about COVID-19 cases,* USA TODAY (Aug. 9, 2020, 6:00 A.M.), https://www.usatoday.com/story/news/investigations/2020/08/09/schools-cite-hipaa-hide-coronavirus-numbers-they-cant-do-that/3323986001/.
[113] *Id.*

that compelling compliance with disease controlling directives violated HIPAA.[114]

Some of these individuals were likely unaware they were discussing the HIPAA Privacy Rule, which the United States Department of Health and Human Services ("HHS") first published in 2000, four years after HIPAA was initially enacted, creating standards under which health plans, health care clearinghouses and certain health care providers (the "covered entities") must protect individually identifiable health information of patients.[115] Under HIPAA, covered entities are limited as to when, how and to whom protected health information ("PHI") belonging to patients may be disclosed.[116] As many would come to learn over the course of the COVID-19 pandemic, HIPAA actually does not confer sweeping medical information privacy protections over any piece of information even loosely related to one's health. Put simply, the Privacy Rule was designed only to protect PHI possessed by a covered entity from being disclosed without patient consent; the rule does not operate as a blanket defense to arm oneself with in the case of someone inquiring about one's medical information on a voluntary basis.[117]

That said, it is alarming that the category of entities that are bound by HIPAA's Privacy Rule disclosure requirements are dwarfed by the category of entities that are *not* covered.[118] It is not prohibited under the Privacy Rule, for example, for a school, employer, store, restaurant, entertainment venue, or similar entity, to inquire about an individual's vaccination status in order to ensure the protection of the general public.[119] On the flip side, the Privacy Rule also does not prevent any individual from voluntarily disclosing his or her own

---

[114] *See, e.g.,* Jon Greenberg, *Marjorie Taylor Greene Says HIPAA Shields Her from Vaccination Questions. It Doesn't.*, POLITIFACT (July 21, 2021), https://www.politifact.com/factchecks/2021/jul/21/marjorie-taylor-greene/marjorie-taylor-greene-says-hipaa-shields-her-vacc/; Camille Caldera, *Fact check: No Mask? You Can Ask Why – It Isn't against HIPAA or the Fourth or Fifth Amendments*, USA TODAY (July 19, 2020, 12:51 PM), https://www.usatoday.com/story/ news/factcheck/2020/07/19/fact-check-asking-face-masks-wont-violate-hipaa-4th-amendment/5430339002/.

[115] *See* U.S. Dep't of Health & Hum. Servs, *The HIPAA Privacy Rule*, HHS.GOV (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[116] *Id.*

[117] *See* Greenberg, *supra* note 114.

[118] *See* 45 C.F.R. § 164.104 (2023) ("Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to . . . a health plan, a health care clearinghouse, a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."); *see also* 45 C.F.R. § 160.103 (2023) ("Covered entity means: (1) a health plan, (2) a health care clearinghouse, (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter".).

[119] U.S. Dep't of Health & Hum. Servs, *HIPAA, COVID-19 Vaccination, and the Workplace*, HHS.GOV (Sept. 30, 2021), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-covid-19-vaccination-workplace/index.html.

health information, including whether or not they have been vaccinated.[120] So, while an employer is free to ask an employee about vaccination status under the Privacy Rule, that employee is not otherwise affirmatively protected from having to disclose that information under the Rule, contrary to what many believed.

Thus, the Privacy Rule is a key component to maintaining information privacy under HIPAA, albeit limited in its application. A closer look at the enactment of HIPAA and the Privacy Rule demonstrates the need to expand its reach since, in the decades that have passed since the law went into effect, massive developments in technology and a sea change in abortion laws have significantly changed the medical privacy needs of society.

Congress passed HIPAA on August 21, 1996, with the intended purposes of improving health insurance coverage continuity and portability in situations where an insured changes employment, thus minimizing and eliminating financial waste, fraud and abuse in health care, and streamlining the overall administration of health insurance in America.[121] Prior to its passage, then-President Bill Clinton pressured Congress in his State of the Union address to pass legislation to ease the numerous hardships suffered by millions of Americans living in fear of the consequences of changing or losing a job, since those events threatened Americans' ability to maintain their desired health insurance across employers.[122] It was estimated at that time by the General Accounting Office that 25 million Americans were at risk of losing health insurance coverage in the event of a change in or loss of job, or were otherwise barred from health insurance coverage due to suffering a pre-existing illness.[123]

To achieve Congress' stated goal of improving health insurance continuity and portability, the legislation necessarily needed to address the complete absence of federal law related to medical information privacy, storage and sharing.[124] Prior to HIPAA's enactment, medical information privacy nationwide was governed through a patchwork of various federal, state and local statutes, regulations, and common laws, which regulated the confidentiality of healthcare information.[125] Not surprisingly, the gaps in coverage between each of the various laws led to confusion and concern among state lawmakers, health care industry members and the insured about how to deal with patient information collection, sharing and processing.[126]

---

[120] *Id.*
[121] Gina Marie Stevens, Cong. Rsch. Serv., RS20934, A Brief Summary of the HIPAA Medical Privacy Rule CRS 2 (2003).
[122] *See* 142 CONG. REC. 9568 (1996) (statement of Rep. Frank Pallone); *see also Id.* (statement of Rep. Greg Ganske).
[123] 142 CONG. REC. 21482 (1996) (statement of Sen. Nancy Kassebaum).
[124] Stevens, *supra* note 121.
[125] *Id.*
[126] *Id.*

Congress, appreciating the rapid modernization of information sharing and increased reliance on electronic storage and transmission, added a provision to the law that would require covered entities to adhere to a set of privacy standards specific to electronically stored information.[127] This standardization provision, titled "administrative simplification", is the root provision from which the HIPAA Privacy Rule derives.[128]

Procedurally, HIPAA authorizes HHS to pass regulations through notice and comment rulemaking to effectuate the Act's privacy objectives. Congress specifically authorized the Secretary of HHS to "adopt security standards" with respect to the electronic processing of health information in order to "ensure the integrity and confidentiality" of such information, and to require certain individuals in possession of health information to adopt safeguards to protect against "any reasonably anticipated unauthorized use[] or disclosure[.]"[129] HIPAA defines health information as "any information, whether oral or recorded in any form or medium" that is:

> created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.[130]

Thus, medical providers, insurance companies, and other covered entities (like business associates contracted by a covered entity) that are in possession of sensitive PHI are required to protect that information from unintended disclosures to third parties without patient authorization.

Notably in 2023, HHS issued a proposed rule to modify the Privacy Rule such that it would prohibit the use or disclosure of PHI to third parties for the purposes of investigating patients seeking, obtaining, providing or facilitating reproductive healthcare, if the patient did so in a state where the healthcare was lawful under state and/or federal law.[131] The prohibition on disclosure would not be absolute—it would permit disclosures in instances where the requestor (e.g., law enforcement) provides an attestation affirming that the intended use of the requested PHI was for purposes unrelated to

---

[127] "One important provision in this bill that has not received much attention is administrative simplification … It aims to cut administrative costs by standardizing the way medical information is electronically stored and transmitted." 142 CONG. REC. 21497 (1996) (statement of Sen. Paul Simon).
[128] 42 U.S.C. §§ 1320d–1320d-9.
[129] 42 U.S.C. §§ 1320d-1, 1320d-2.
[130] *Id.* at § 1320d-4.
[131] HIPAA Privacy Rule to Support Reproductive Health Care Privacy, 88 Fed. Reg. 23506 (Apr. 17, 2023).

investigations into lawfully obtained reproductive healthcare.[132] The proposed rule was HHS' response to an executive order from President Biden titled Protecting Access to Reproductive Healthcare Services, in which the President ordered his agencies to examine ways to strengthen access to abortion after the *Dobbs* opinion.[133] Over two dozen state attorneys general wrote in support of HHS' proposed rule, and specifically applauding the rule's expanded notice requirements.[134] As of March 2024, HHS has yet to finalize the proposed Privacy Rule modification.

Overall the proposed rule would protect patients receiving lawful abortions from having those associated health records obtained by law enforcement in attempts to initiate criminal or administrative proceedings against them for obtaining lawful healthcare.[135] However, the proposal overlooks one flaw in the existing Privacy Rule: the definition of "covered entities" is too narrow. As it stands, the rule does not extend to software developers that create and publish apps designed to track user health, like menstrual cycles, heart rate, insulin levels, medication schedules, fitness and more.[136] Perhaps if an app developer is working on behalf of a covered entity; that is, if the developer is a business associate of a covered entity and creates, receives, maintains or transmits PHI, then it may be required to comply with the Privacy Rule.[137] But a large number of health-based mobile app developers do not fall within this limited business associate exception, therefore users voluntarily providing PHI to apps do not realize that that information is not subject to HIPAA's privacy. This is why HHS should take additional steps to expand the definition of covered entities to account for the massive network of app developers operating at the intersection of health information and technology.[138]

---

[132] *Id.* at 23516.

[133] Exec. Order No. 14,076, 3 C.F.R. § 400 (2023) at 401(asking the Secretary of HHS to consider modifying regulations implementing HIPAA, and any other relevant statutes, to "strengthen the protection of sensitive information related to reproductive healthcare services.").

[134] State Attorneys General, Comment Letter on HIPAA Privacy Rule to Support Reproductive Health Care Privacy (June 16, 2023), https://downloads.regulations.gov/HHS-OCR-2023-0006-0188/attachment_1.pdf.

[135] HIPAA Privacy Rule To Support Reproductive Health Care Privacy, 88 Fed. Reg. 23506, 23530 (Apr. 17, 2023) (to be codified at 45 C.F.R. pts. 160, 164).

[136] *See* Jeannie Baumann, *Fertility Apps Bound by Weak Disclosure Rules in Post-Roe World*, BLOOMBERG L. (May 18, 2022, 5:35 AM), https://news.bloomberglaw.com/pharma-and-life-sciences/fertility-apps-bound-by-weak-disclosure-rules-in-post-roe-world.

[137] Health & Hum. Servs. Off. For Civ. Rts., *Health App Use Scenarios & HIPAA,* U.S. DEP'T HEALTH & HUM. SERVS. (Feb. 2016), https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf.

[138] Furthermore, given Congress' observation that HIPAA would account for the rapid modernization of technology increasing the rate at which medical information was electronically exchanged, lawmakers should similarly consider passing legislation amending

Health tracking apps have many benefits as tools to monitor and take control of one's health and wellness, but app developers are not medical professionals, are not bound by HIPAA and have no duty under the Privacy Rule to obtain a user's consent prior to disclosing the collected information. Because HIPAA's Privacy Rule does not extend to app developers, it is the user's obligation to understand what, if any, information will be kept private. And while apps and websites sometimes declare privacy policies, as discussed above, the policies are almost impossible for a layperson to read and understand.[139] One study by the UK-based Organization for the Review of Care and Health Apps ("ORCHA") determined that 84% of the twenty-five apps reviewed enabled sharing of personal and sensitive health data with third parties.[140] The group warned that, even though names and addresses of users may not be included in the bulk of the data being shared, users can just as easily be identified through an IP address, thus eliminating user anonymity altogether.[141]

The pervasiveness of the electronic distribution of millions of users' personal health information cannot be overstated. In an effort to combat this widespread data sharing, activist organizations, such as Fight for the Future, are working to hold healthcare tech companies accountable for their data practices.[142] One report shockingly revealed that the popular prescription drug app Drugs.com shared its user data with more than 100 third-party entities, including advertising companies.[143] It was further discovered that the app had even sent a user's first and last name to a third party, which the company claimed was unintentional.[144]

Some may argue that the information obtained by authorities from the Facebook messages exchanged in the Nebraska abortion criminal case could constitute PHI protected by HIPAA in a healthcare context. But, as shown, Meta is not a covered entity, and investigators were not requesting PHI; thus, the company was not remotely close to triggering HIPAA's limitation on the disclosure of sensitive personal health information of its users.[145] Still, the

---

HIPAA to update the definition of covered entities in order to fully capture the myriad technological advances in the decades since HIPAA was first enacted.

[139] Fowler et. al., *supra* note 97.

[140] ORCHA, *84% of Period Tracker Apps Share Data with Third Parties*, ORCHA (July 21, 2022), https://orchahealth.com/84-of-period-tracker-apps-share-data-with-third-parties/.

[141] *Id.*

[142] *See Google: Stop Endangering Abortion Seekers*, FIGHT FOR FUTURE.ORG, https://www.fightforthefuture.org/actions/google-endangers-abortion-seekers (last visited May 14, 2024) (online petition calling on Google to halt its collection of user location data).

[143] Tatum Hunter & Jeremy B. Merrill, *Health Apps Share Your Concerns with Advertisers. HIPAA Can't Stop It.*, WASH. POST (Sept. 22, 2022, 10:26 AM), https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy/.

[144] *Id.*

[145] *See* 45 C.F.R. §§ 164.501-534.

Privacy Rule in its current form does allow covered entities to disclose in instances where the requestor is executing a search warrant or has a court order for the information.[146]

The foregoing illustrates that app developers in the health sector are engaged in mass collection of private information, and are largely unwilling to alter their approach in what they collect, how they collect it and how they may share it even after the shift in the political and legal landscapes post-*Dobbs*.[147] HHS has authority to regulate this collection of health data, and it must affirmatively do so. HHS should modify the HIPAA Privacy Rule to expand the definition of covered entities to include developers of web-based and mobile applications that do not fall within the business associate exception, but that still collect and store PHI. This would ensure that individuals would have some control, or at least a better understanding of how to protect their medical information. Given the advancements in health-related technology since HIPAA was first enacted, modifying the Privacy Rule to increase the reach of its protection is a necessary step towards shoring up data privacy in a post-*Dobbs* society.

B. Federal Trade Commission: reports, investigations and enforcement

Apart from the order to HHS to modify HIPAA's privacy regulations, President Biden directed other federal agencies to explore actions that would "protect healthcare service delivery and promote access to critical reproductive services, including abortion." [148] On the issue of patient privacy, the President highlighted potential risks associated with "the transfer and sale of sensitive health-related data and by digital surveillance related to reproductive healthcare services."[149] To specifically combat this threat, the Chair of the Federal Trade Commission was ordered to conduct efforts, under the Federal Trade Commission Act ("FTC Act"),[150] "to protect consumers' privacy when seeking information about and provision of reproductive healthcare services."[151]

The FTC has investigative, enforcement and rulemaking authority, each of which contributes to the agency's long history of researching and formulating data privacy policy recommendations for lawmakers, and

[146] 45 C.F.R. § 164.512(f)(1)(ii)(A) (2023).
[147] Amy Keller & David Straite, *Dobbs Ruling Means It's Time To Rethink Data Collection*, LAW 360 (June 30, 2022, 6:00 PM), https://www.law360.com/articles/1507779/dobbs-ruling-means-it-s-time-to-rethink-data-collection.
[148] Exec. Order No. 14,076, 87 Fed. Reg. 42053 (July 8, 2022).
[149] *Id.* at 42054.
[150] *See* 15 U.S.C. § 41 *et seq.* (establishing the Federal Trade Commission).
[151] Exec. Order No. 14,076, 87 Fed. Reg. at 42054.

bringing authorized enforcement actions to protect Americans' data privacy on the internet.[152] Since the mid-1990's, when the internet's popularity increased exponentially, the FTC issues regular reports to Congress documenting concerns the agency has about data privacy and the private sector's information practices.[153] Such concerns have primarily rested on the fact that technological advancements persistently make it easier for companies to track, collect and share user information, while laws and regulations fail to match their pace.[154]

After the President's executive order on abortion, the FTC released a statement informing the public about data collection, identifying the widespread frequency of the practice.[155] As the agency noted, a majority of consumers have no idea what happens to their information after they volunteer it online.[156] But, as the FTC pointed out, commonly used devices and software, such as smartphones, tablets, computers, wearable fitness trackers, internet browsers, and "smart home" artificial intelligence assistants like Amazon's Alexa and Apple's Siri are constantly collecting and storing user data.[157] Many consumers might suppose that their information is stored on a company server or cloud somewhere, when in reality the companies collecting data actually proceed to sell it to interested third-parties, which are often data brokers that process and develop aggregate consumer data for other lucrative purposes.[158]

---

[152] *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/mission/enforcement-authority (last updated May 2021).

[153] *See, e.g.*, FED. TRADE. COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[154] See generally *id.*

[155] See Kristin Cohen, Location, Health and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data, FED. TRADE COMM'N: BUS. BLOG (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[156] *Id.* ("The marketplace for this information is opaque and once a company has collected it, consumers often have no idea who has it or what's being done with it. After it's collected from a consumer, data enters a vast and intricate sales floor frequented by numerous buyers, sellers, and sharers.").

[157] *Id.*

[158] *See Location Data Brokers*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/location-data-brokers (last visited May 14, 2024). Data brokers generally are companies that collect information from hundreds of millions of people using trackers built into apps installed on consumer mobile devices. *Id.* The information gathered often includes user location, but may also consist of other identifiable markers like user age and sex. *Id.* Data brokers take advantage of gaps in privacy laws in order to obtain and sell data en masse to a variety of buyers including advertisers, developers, and even government law enforcement agencies, with no control over how those buyers then use the data. *Id.*

As various FTC reports demonstrate, the issue of mass collection and sale of consumer information to third-parties is of paramount importance to the Commission.[159] In 2014, the FTC issued a sweeping report to Congress compiling findings from a year's long study of nine different data brokers, proposing several recommendations for legislative action to try and curtail the shadowy business practices of "Big Data."[160] The report thoroughly described the mechanisms by which data brokers acquire data, how they develop data into a useful product, who they provide their products to, and how they do it.[161]

According to the report, data brokers begin their process largely by relying on indirect sources to gather data, including government sources, commercial sources and other are publicly available sources.[162] With respect to health-related information, data brokers have tended to obtain information from financial services companies, which offer data about certain health-related purchases.[163] Brokers then process data and allocate users into different categories based on personal interests (e.g., "Dog Owner", "Winter Activity Enthusiast" or "Mail Order Responder").[164] Some data brokers go so far as to categorize users based on sensitive health-related information, such as "Expectant Parent," "Diabetes Interest," and "Cholesterol Focus."[165] Isolating the data into groups based on interests creates a useful product that commercial businesses then purchase from data brokers to help those companies improve their targeted marketing efforts.[166]

In the FTC's 2014 report, the agency urged Congress to pass legislation "that would enable consumers to learn of the existence of activities of data brokers" and to "provide consumers with reasonable access to information about them" in the possession of data brokers.[167] Yet, as this article points out, Congress has not so far passed any such legislation. The FTC recently took matters into its own hands, however, and issued a rulemaking proposal that signaled its intent to implement regulations to control consumer information sharing practices through its enforcement authority.

---

[159] Exec. Order No. 14,076, 87 Fed. Reg. at 42054.
[160] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[161] *Id.* at 10.
[162] *Id.* at 11.
[163] *Id.* at 13-14. This data is generally available for collection since "[h]ealth-related purchases are not covered under [HIPAA] . . . [t]he data brokers are not covered entities under HIPAA . . . ." *Id.* at 14, n. 41.
[164] *Id.* at 47.
[165] *Id.*
[166] FED. TRADE COMM'N, *supra* note 153, at 47.
[167] *Id.* at 49.

In its Advanced Notice of Proposed Rulemaking ("ANPR"), the FTC requested public comment on the "prevalence of commercial surveillance and data security practices that harm consumers."[168] The ANPR specifically asked the public to weigh in on "whether [the FTC] should implement new trade regulation rules" concerning the ways that companies "collect, aggregate, protect, use, analyze and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive."[169] The FTC is authorized by Congress to declare unlawful any "unfair or deceptive" act or practice that is likely to cause "substantial injury" to consumers that is "reasonably unavoidable" and is not outweighed by any potential consumer benefit, and may do so by adopting regulations to address these unlawful practices.[170] The ANPR identified multiple instances in which the FTC had already launched enforcement actions against various entities for violations related to data privacy and security, in particular for violations of the FTC Act stemming from sharing private health-related data with third-parties.[171] By the time the comment period ended, the FTC received over 11,000 public responses to the ANPR.[172]

In the ANPR, the FTC provided several reasons to support its decision to implement new regulations to reign in commercial data surveillance.[173] First, the FTC Act limits the agency's ability to seek civil penalties under Section 5 for first-time violations, thus hindering the overall strength of first-time enforcement actions against large companies likely to be in possession of a vast amount of consumer data.[174] Second, even though the FTCA authorizes the FTC to order an injunction on conduct that violates Section 5, merely enjoining violative conduct is not always an adequate remedy.[175] Third, monetary relief that is available under the FTC Act is not always clearly assessable, given the complex nature of the types of injury that arise from unmitigated data breaches.[176] Lastly, the FTC is limited in resources to dedicate to investigating the vast number of data security practices currently

---

[168] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (Aug. 22, 2022) (to be codified at 16 C.F.R. pt. 1).
[169] *Id.*
[170] Federal Trade Commission Act § 45(n).
[171] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51278.
[172] Fed. Trade Comm'n, *FTC Seek Comments on Trade Regulation Rule on Commercial Surveillance and Data Security, R111004,* REGULATIONS.GOV, https://www.regulations.gov/docket/FTC-2022-0053 (last visited May 14, 2024).
[173] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51280.
[174] Federal Trade Commission Act § 45(l).
[175] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51280.
[176] *Id.* at 51280-81.

employed by data industry members.[177] In light of these reasons, the FTC says, implementing new regulations on consumer surveillance and data privacy practices is the most feasible way to both provide clarity to businesses about what sort of privacy protections are required, and allow the FTC to more predictably enforce the FTC Act as it pertains to consumer data privacy.[178]

One of FTC's recent enforcement actions demonstrates precisely the reason that mass proliferation of consumer health-related data warrants regulatory action. In 2021, the FTC settled claims against Flo Health Inc., a femtech company behind Flo, a fertility-tracking app.[179] The FTC alleged the company frequently shared sensitive health-related data of millions of its users with third-party marketing and analytics firms, as well as Meta and Google.[180] In its complaint, the FTC contended that Flo's practice of sharing users' intimate reproductive health information with third parties was done without first notifying users, and denied users the opportunity to opt-out of data sharing.[181] This, the FTC argued, was unlawful conduct that constituted a violation of Section 5 of the FTC Act.[182] The complaint went further, alleging Flo repeatedly assured its users that their data would be kept private and only used by Flo itself to help improve the app's service and performance.[183] In reality, the complaint says, Flo was disclosing sensitive user information via specialized software (known as software development kits, or SDK's[184]) built into the Flo app that gathered user data and fed it directly to third-party firms for profit.[185]

Not only was Flo's ubiquitous data sharing hidden from its users, it also directly violated the terms of use of several of the third-party's that the company was delivering user data to, per the complaint.[186] Flo operated in this manner for years until an article by the Wall Street Journal reported on the practice, and on nearly the same day the Journal's article was published,

---

[177] *Id.* at 51281.
[178] *Id.*
[179] FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others, FED. TRADE. COMM'N (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.
[180] *Id.*
[181] Complaint at 7-8, *In re* Flo Health, Inc., No. C-4747 (F.T.C. issued June 17, 2021).
[182] *Id.* at 11.
[183] *Id.* at 3.
[184] *See* Sara Morrison, *The Hidden Trackers in Your Phone, Explained*, VOX (July 8, 2020, 10:30 AM), https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location. Software development kits, or SDK's, are programs that app developers embed into their app software to collect user data. *Id.* The app developers profit off that user data by transferring or selling it to marketing and analytics firms, or companies like Facebook, Amazon, or Google. *Id.*
[185] Complaint at 4-5, *In re* Flo Health, Inc., No. C-4747 (F.T.C. issued June 17, 2021).
[186] *Id.*

Flo discontinued its practice.[187] Ultimately, the FTC and Flo reached a settlement in which the company agreed to adopt improved privacy policies—among them were various notice and consent requirements in order to properly notify its users of the company's data collection and sharing practices.[188]

In another enforcement proceeding, the FTC charged an ovulation tracking app with deceiving users about its data sharing practices, and violating the Health Breach Notification Rule.[189] Among the allegations, the FTC claimed Premom shared sensitive personal information with third-parties based out of China and Google, without the consent or knowledge of its users.[190] As with Flo, the FTC claimed Premom used SDK's from third-party advertisers that collected user data and was used to inform other companies' targeted advertising.[191] The types of sensitive information shared included users' sexual and reproductive health, pregnancy status and other details about physical health conditions.[192]

There is a line that can be drawn directly from the Flo and Premom cases to the FTC's ambitious ANPR on the issue of unmitigated commercial data surveillance. Flo and Premom's enforcement proceedings are clear demonstrations of how mobile-app users' data is collected, stored, transferred and sold to third parties, without user knowledge or consent. With the ANPR, the FTC is rightfully signaling that it has a keen interest in pursuing the appropriate next steps to strengthen its ability to investigate companies' unfair and deceptive data sharing practices, and initiate enforcement actions to the fullest extent allowed under the FTC Act.

C. Other Agency Action After Dobbs

Other federal agencies have acted to address changes in the laws on abortion after *Dobbs*. For example, the United States Department of Justice Office of Legal Counsel ("OLC") issued a legal opinion to the United States Postal Service ("USPS") pronouncing that, under certain circumstances, mailing abortifacient drugs is not prohibited under federal law.[193] Specifically,

---

[187] *Id.* at 2.
[188] Decision & Order, *In re* Flo Health, Inc., No. C-4747 (F.T.C. issued June 17, 2021).
[189] *Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order*, FED. TRADE COMM'N (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc.
[190] *Id.*
[191] *Id.*
[192] *Id.*
[193] Application of the Comstock Act to the Mailing of Prescription Drugs That Can Be Used for Abortions, 46 Op. O.L.C. 1-2 (2022).

the mailing, delivery or receipt by mail of mifepristone or misoprostol, the two prescription drugs used for self-induced abortion, is not prohibited under federal law so long as the sender does not intend for the recipient to use the drugs unlawfully.[194] Conservative state attorneys general strongly opposed the OLC's opinion, and advised major pharmacy retailers that, as abortion remains illegal in their states, and pharmacies should be cautious about distributing abortion medication to their states' citizens via the USPS.[195] Since that time, two major retailers have announced their intent to dispense mifepristone in states where it is legal to do so, although it was not clear from their announcement whether the retailers would engage in mail-order prescriptions of the drug.[196]

This debate over the legality of mailing abortifacient drugs is extremely relevant in the context of online data privacy, since an outstanding number of people use internet-based organizations like AidAccess[197] and PlanC[198] to search for and order these medications online. Investigations revealed more reason to be concerned about online ordering: out of 11 online abortion pill retailers analyzed, 9 used third-party web trackers to collect user information, like browsing history, cross-site activity, and device geolocation.[199] One of the third-party trackers used was Google Analytics, and in response to the investigation, Google stated the data it received from the online abortion drug retailers was aggregated and obfuscated—meaning that it was not possible to identify individuals in the data set.[200] Still, that data set, if in the hands of prosecutors in states taking the position that abortion drugs transmitted via U.S. mail are illegal, could be strong evidence in a criminal case.

Agency actions like those described above have their advantages, like the speed at which they can proceed, the breadth of agency expertise available to inform reasoned decision-making, and the ability for the public to provide comments that hopefully aid agencies in finalizing comprehensive regulations that meet the moment. The problem with agency actions is that they are subject to legal challenges, and they are easy to roll back with a change in

---

194 *Id.*

195 *See* Letter from Andrew Bailey, Att'y Gen. Mo., to Danielle Gray, Exec.Vice President, Walgreens Boots All., Inc. (Feb. 1, 2023) (on file with the Office of the Attorney General for the State of Missouri).

196 Jaclyn Diaz & Alina Selykuh, *CVS and Walgreens to start dispensing abortion pill in states where it's legal,* NPR (Mar. 2, 2024, 2:19 PM), https://www.npr.org/2024/03/01/1235265078/ abortion-pill-cvs-walgreens-mifepristone.

197 AIDACCESS, https://aidaccess.org/en/ (last visited May 14, 2024).

198 PLAN C, https://www.plancpills.org/ (last visited May 14, 2024).

199 Jennifer Gollan, *Websites Selling Abortion Pills Are Sharing Sensitive Data With Google,* PROPUBLICA (Jan. 18, 2023, 5:00 A.M.), https://www.propublica.org/article/websites-selling-abortion-pills-share-sensitive-data-with-google.

200 *Id.*

presidential administration. These reasons demonstrate why it is imperative for Congress to pass a robust data privacy law to address the current gaps in legislation that enable exploitive use of personal and private data.

D. Federal Legislative Proposals to Combat Rampant Data Collection Practices

The motivation for this article is the complete absence of federal law to uniformly regulate how private corporations and governments collect, store or share user data in the United States.[201] And now that abortion is illegal in nearly half the states, user data privacy is more important than ever. Every second of every day, companies are collecting endless streams of user information to be used in a variety of lucrative ways, such as crafting targeted advertisements,[202] conducting user experience research,[203] and performing mass selloffs to third-parties like data brokers and government agencies.[204] Some states have enacted, or have attempted to enact, laws that restrict or limit the ways that consumer data can be collected, stored, transferred or sold.[205] However, the federal government is lagging behind.

In August 2022, a bipartisan group of representatives introduced the American Data Privacy and Protection Act ("ADPPA"), seeking to "provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement."[206] The bill did not deem data sharing plainly unlawful; rather, the overarching purpose of the bill was to create and expand transparency on the data sharing practices, and to require that data holders employ safeguards to ward off data breaches.[207] With respect to the latter, the bill contained a provision that covered entities "establish, implement, and maintain reasonable administrative, technical, and

---

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

[202] Natasha Singer, *This Ad's for You (Not Your Neighbor)*, N.Y. TIMES, https://www.nytimes.com/2022/09/15/business/custom-political-ads.html (last updated Sept. 20, 2022).

[203] *See* Meghan Wenzel, *Collecting Data Is One Thing—Acting on It Is Another*, UX MATTERS (Sept. 9, 2019), https://www.uxmatters.com/mt/archives/2019/09/collecting-data-is-one-thingacting-on-it-is-another.php.

[204] *See supra* Part II.C.

[205] *See* Andrew Folks, *US State Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last updated Mar. 15, 2024). At the time of this writing, only 15 states have comprehensive privacy laws in effect that govern the use of personal information. *Id.* Another 15 have introduced privacy bills that are currently going through the legislative process. *Id.*

[206] H.R. REP. NO.117-669, at 1 (2022).

[207] See generally *id.*

physical data security practices and procedures to protect and secure covered data against unauthorized access and acquisition."[208] On the transparency issue, covered entities would be required to "make publicly available, in a clear, conspicuous, not misleading, and easy-to-read and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the data collection, processing, and transfer activities of the covered entity."[209]

The bill was voted out of committee with strong bipartisan support; however, a major dispute developed concerning the bill's state law preemption provision.[210] The bill expressly preempted states from "adopt[ing], maintain[ing], [or] prescrib[ing]" any law which would be covered by the provisions of the ADPPA.[211] The problem: this provision directly conflicted with the ability of states that have their own data privacy legal framework to enforce those laws, such as California.[212] In a press release, California Governor Gavin Newsom expressed frustration with the ADPPA's attempt to undermine the California Consumer Privacy Act (CCPA), which provides more rigorous protection than the ADPPA purports to offer.[213] In effect, the ADPPA would set a "federal ceiling," whereas most federal legislation aims to set a "federal floor" that states are free to exceed with more protective regulations.[214]

In addition to lawmaker disagreements about the ADPPA, five of the most prominent commercial data brokers tirelessly lobbied against the bill and other proposals similar to it.[215] Not surprisingly, the lobbyists included tech titans like Microsoft and Amazon, as well as consumer credit reporting companies like TransUnion and Experian.[216] The companies demanded certain exemptions be worked into the bill; for example, the lobbyist groups wanted exceptions written in for entities engaging in data sharing of de-identified information.[217] De-identified data is frequently used in medical research and healthcare studies to collectively examine the status and results

---

[208] *Id.* § 208(a)(1).
[209] *See id.* § 202(a).
[210] Press Release, Gavin Newsom, Governor, State of California, Governor Newsom, Attorney General Bonta and CPPA File Letter Opposing Federal Privacy Preemption (Feb. 28, 2023) (on file with author).
[211] H.R. REP. NO. 117-669 § 404(b)(1) (2022).
[212] *See US State Privacy Legislation Tracker: Comprehensive Consumer Privacy Bills*, IAPP, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf (last updated Mar. 15, 2024).
[213] NEWSOM, *supra* note 210.
[214] *Id.*
[215] Alfred Ng, *Privacy Bill Triggers Lobbying Surge by Data Brokers*, POLITICO (Aug. 28, 2022, 7:02 AM), https://www.politico.com/news/2022/08/28/privacy-bill-triggers-lobbying-surge-by-data-brokers-00052958.
[216] *Id.*
[217] *Id.*

of large groups of patients.[218] De-identified data sharing is a practice that HHS tolerates, and at one time the Department released guidance on the proper use of de-identified data in medical research so that entities could satisfy HIPAA's privacy requirements.[219] But privacy advocates argue that when one type of PII is left in one data set (e.g., location or search history), that data could theoretically enable re-identification when compiled with another dataset (e.g., phone call logs or customer lists), meaning a data analyst could potentially identify an individual out of combined group datasets.[220]

In any event, it is unlikely at this point that lawmakers would reach consensus on the current form of the ADPPA given the concerns raised by California and interested lobbyists that oppose the legislation. Still, the ADPPA was one of the most ambitious pieces of data privacy legislation to be introduced in recent years, and would have been a tremendous leap towards closing the gap between the stalling U.S. and its global counterparts that already have robust data privacy laws and regulations.[221]

Another recent attempt at federal legislation, aimed specifically at establishing protections for information related to personal reproductive and sexual health, was the My Body, My Data Act of 2023, which would vest the FTC with authority to enforce violations of the law as well create a private right of action for individuals.[222] It would prohibit the collection, retention, use or disclosure of personal reproductive or sexual health information, except in instances where an individual provided express consent, or where the information was necessary to deliver a product or service to an individual requesting it.[223] In the latter case, individuals would have the right to access their collected information, as well as request its deletion.[224] Regulated entities would be required to disclose their privacy policies plainly on their website.[225] Remarkably, the bill would not apply to entities governed by HIPAA's privacy rule regulations; instead, the regulated entities would consist of any person, partnership or corporation engaged in activities in or affecting

---

[218] U.S. Dep't Health & Hum. Servs., Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (2012).
[219] *Id.* at 4.
[220] Boris Lubarsky, Technology Explainers, *Re-Identification of "Anonymized" Data,* 1 GEO. L. TECH. REV. 202, 203 (2017).
[221] *See* Danny O'Brien, *The Year of the GDPR: 2018's Most Famous Privacy Regulation in Review*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Dec. 28, 2018), https://www.eff.org/es/deeplinks/2018/12/year-gdpr-2018s-most-famous-privacy-regulation-review. The European Union passed the General Data Protection Regulation (GDPR), which has been heralded by many as a strong example of how to defend data privacy online. *Id.*
[222] My Body, My Data Act of 2023, H.R. 3420, 118th Cong. § 6 (1st Sess. 2023).
[223] *Id.* at § 2(a).
[224] *Id.* at § 3(a), (c).
[225] *Id.* at § 4(a)-(b).

commerce, as defined under Section 4 of the FTC Act.[226] This carve-out seemingly still leaves room for HHS to amend its privacy rule to expand the definition of covered entities to close any gaps in coverage.[227] And unlike the ADPPA, the My Body, My Data Act would not preempt states from implementing their own stronger privacy protections as it pertains to reproductive and sexual health privacy.[228]

The My Body, My Data Act would create a new national standard to protect individuals' private reproductive health data by minimizing the amount of data that is collected, and prohibiting that information from being disclosed.[229] The bill received widespread support from data privacy advocacy groups, abortion rights organizations and gender equality advocates.[230] The bill has not made any advancements since it was introduced in May 2023, and even Congresswoman Jacobs, who introduced the bill in the U.S. House, was skeptical about whether republicans in the House or the Senate would be on board.[231] Still, Jacobs believed the proposed bill would serve as a model from which she hopes states will draft their own legislation in order to combat excessive data collection in the healthcare space.[232]

III. CIRCUMVENTING FOURTH AMENDMENT PRIVACY PROTECTIONS

Even in instances where companies embrace strong privacy policies to protect user data from unnecessary third-party disclosure, lawful requests from law enforcement usually result in companies setting aside user privacy. The Fourth Amendment protects individuals from warrantless government search and seizure of their property or person when the individual has a subjective expectation of privacy that society is willing to accept as reasonable.[233] While Fourth Amendment jurisprudence has evolved over time as society has modernized and technology has advanced, individuals generally do not enjoy a Fourth Amendment right to privacy over digital information

---

[226] *Id.* at § 7(6).
[227] *See supra* Part II.A.
[228] H.R. 3420 § 9(b)(2).
[229] Press Release, Sara Jacobs, Congresswoman, House of Representatives, Rep. Sara Jacobs Leads Reintroduction of My Body, My Data Act to Protect Reproductive and Sexual Health Data (May 17, 2023) (on file with author).
[230] Hayley Tsukayama, *Support the "My Body, My Data" Act,* ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (May 18, 2023), https://www.eff.org/deeplinks/2023/05/eff-supports-my-body-my-data.
[231] Emily Tisch Sussman, *This Bill Wants to Stop Anti-Abortion Groups From Getting Your Private Data. Period,* MARIE CLAIRE (July 13, 2022), https://www.marieclaire.com/politics/abortion-and-period-trackers-my-body-my-data-bill/.
[232] *Id.*
[233] Katz v. United States, 389 U.S. 347, 361 (1967) (Douglas, J., concurring).

they volunteer to third-parties—like ISP's and internet websites.[234] As a result, the U.S. government has routinely engaged in the practice of purchasing Americans' personal information from data brokers, entirely outside of the judicial processes that the Fourth Amendment requires.[235] The government's habit of obtaining Americans' information in this way completely circumvents the constitutional requirements.[236] Some have deemed the practice the "reverse search warrant," since, generally, the information obtained in these bulk data purchases would only help law enforcement locate potential suspects of crimes, as compared to a search warrant's inherent purpose of investigating an already identified.[237] Still, this digital dragnet surveillance practice of the government has yet to be held by the courts to violate the Fourth Amendment.[238]

A. The Fourth Amendment is Not For Sale

Congress, looking to remedy the problems associated with government surveillance, introduced the Fourth Amendment Is Not For Sale Act, which would restrict the government's ability to conduct warrantless seizures of various types of user data and information from data brokers and other third parties that receive or possess bulk user data or information.[239] Specifically, the bill would prohibit a law enforcement agency of a governmental entity from purchasing through a third-party any information that was disclosed to and collected by that third-party either from a user himself, or through an intermediary source.[240] In addition to this strict prohibition on purchasing user information, the bill would further prohibit any illegitimately obtained information in violation of the law from being received as evidence in any trial or other proceeding before a court.[241] In effect, an agency like the Drug

[234] United States v. Miller, 425 U.S. 435, 443 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." (citing United States v. White, 401 U.S. 745, 751–52 (1971))); Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").
[235] Press Release, ACLU New York, New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data (July 18, 2022) (on file with author).
[236] *See id.*
[237] *Reverse Search Warrants,* NAT'L ASS'N CRIM. DEF. LAWS. (Nov. 2, 2022), https://www.nacdl.org/Content/Reverse-Search-Warrants-NY.
[238] Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole,* BRENNAN CTR. FOR JUSTICE (Feb. 13, 2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole.
[239] Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. (as introduced in the Senate, Apr. 21, 2021).
[240] *Id.* at § 2.
[241] *Id.* at § 2(4).

Enforcement Administration or the Federal Bureau of Investigation, would be prohibited from buying user information from commercial data brokers to aid themselves in an investigation, and if the agency were to proceed with purchasing the information in violation of the law, that information would be forbidden from being used to aid any prosecution.

Elsewhere, the bill would also prohibit sharing the purchased consumer data across government agencies.[242] This prohibition on inter-governmental transfer may directly undermine some of the existing government contracts with private entities that provide Americans with easy and accessible ways to access government agency websites. For example, Login.gov[243], a website that provides individuals with the option to create universal, secure single sign-on credentials to access various participating government agencies' websites, through which it verifies user information by relying on private-sector data brokers, could be hampered by this bill in its ability to share information across the government agencies it services.[244]

In order to use Login.gov, a user must create a single login credential that will be used across multiple government agency websites, including the Small Business Administration, the Office of Personnel Management, the Social Security Administratio and more.[245] To create an account, a user must volunteer certain specific and personally identifying information that operates both as a way for Login.gov to confirm the user is in fact the person they claim to be, and as a form of fraud detection.[246] Two principal forms of personally identifying data that Login.gov accepts are facial recognition and fingerprint touch unlock, which are each uniquely specific to each individual and difficult if not impossible to replicate.[247] However, it was eventually reported that the party responsible for conducting the identity verification for users of Login.gov was not the government—it was a group of private-sector data brokers.[248]

The idea of a streamlined single sign-on process to access government websites is attractive: a convenient tool that reduces the need for users to

---

[242] *Id.* at § 2(3).
[243] *What is Login.gov?*, LOGIN.GOV, https://login.gov/what-is-login/ (last visited May 14, 2024).
[244] *See* Alfred Ng, *Privacy Bill Triggers Lobbying Surge by Data Brokers*, POLITICO (Aug. 28, 2022, 7:02 AM), https://www.politico.com/news/2022/08/28/privacy-bill-triggers-lobbying-surge-by-data-brokers-00052958.
[245] *Id.*
[246] *Authentication Methods*, LOGIN.GOV, https://login.gov/help/get-started/authentication-options/ (last visited May 14, 2024).
[247] *See id.*
[248] Alfred Ng, *Data brokers raise privacy concerns – but get millions from the federal government,* POLITICO (Dec. 21, 2022, 4:30 AM), https://www.politico.com/news/2022/12/21/ data-brokers-privacy-federal-government-00072600.

create dozens of sign-on credentials for a variety of government websites; however, a closer look reveals that government contracts with some of the private sector entities that perform the identity verification services pose significant data privacy concerns. For example, LexisNexis, a highly data-driven company that operates a robust catalogue of personally identifying information for millions of properties, individuals, and businesses, is directly associated with Login.gov.[249] In fact, LexisNexis was awarded a contract by the General Services Administration to provide digital identity verification for Login.gov as recently as December 2021.[250] LexisNexis therefore provides a valuable service to government agencies, functioning as a digital identity verification tool in order to allow individuals to engage with various government programs.

In turn, however, LexisNexis and other popular information aggregators conduct their own mass data assembly activities, aggregating things like names, social security numbers, addresses, and in some cases, even facial recognition.[251] In response to concerns about the efficacy and security of ID.me, a digital identity verification company contracted by the government to perform facial recognition identity confirmation, members of the House Oversight Committee launched an investigation citing inaccuracies in the software that led to delays in some Americans' abilities to receive pandemic assistance benefits.[252] Because no federal laws regulate the use of facial recognition technology, there are no rules in place that govern how companies must protect stored images of users' faces. After a rise in complaints from advocacy groups and members of Congress, ID.me agreed it would discontinue its use of facial recognition technology.[253]

This background highlights several ways the federal government participates in the mass collection, sale, and transfer of user data, and confirms that there is a desperate need for legislation to regulate data privacy. The Fourth Amendment Is Not for Sale Act would seemingly prevent a prosecutor in an abortion-hostile state like Texas or Oklahoma from simply purchasing mass amounts of user data from commercial data brokers to try and build a case against someone for obtaining an abortion. Contrast this, however, with the judicial process that investigators in the Nebraska abortion case followed in order to obtain the Facebook messages of the women charged. Yet even if investigators did not obtain a warrant, it is unlikely that Facebook would have

---

[249] *See* Press Release, LexisNexis Risk Solutions, CALIBRE Systems, Inc. and LexisNexis Risk Solutions Team up to Strengthen Secure Access to Government Agencies Through the Login.gov Single Sign-on Solution (Dec. 6, 2021) (on file with Cision PR Newswire).
[250] *Id.*
[251] *See generally* Cat Zakrzewski, *House Lawmakers Launch Investigation of Face-Scan Contractor ID.me*, WASH. POST (Apr. 14, 2022, 12:05 PM), https://www.washingtonpost.com/technology/2022/04/14/idme-facial-recognition-investigation/.
[252] *Id.*
[253] *Id.*

made the messages available for purchase to the investigators, according to the websites' privacy policies.[254]

B. Geofencing

Another prominent method of data collection that has been the subject of Fourth Amendment challenges, and is frequently used by companies like Google, is "geofencing." As the name suggests, the practice involves companies collecting user location data off of their mobile devices through virtual "fences" erected around certain locations—the data collection is triggered when a device enters or exits the virtual boundaries of the geofence.[255] This creates an environment where, even a Google search for an address where a crime happens to take place could render you a suspect, just based on your search results appearing in the dataset obtained by police.[256]

Geofencing is also extremely useful for targeted marketing and advertising, and anti-abortion organizations are no stranger to those benefits. In Massachusetts, for example, an advertising agency was accused of using geofencing technology in 2015 to target women entering abortion clinics, sending them targeted smartphone ads with messages like "You Have Choices."[257] The Massachusetts Attorney General argued the company used geofencing technology in five cities outside of the state of Massachusetts, and had the capability of performing the practice in Massachusetts as well.[258] The advertising firm responded that it had been approached by a Christian adoption agency and a California-based network of crisis pregnancy centers with the proposal to target advertisements at "abortion-minded women" visiting reproductive health clinics.[259] In a win for privacy rights, the Massachusetts Attorney General secured a settlement whereby the

---

[254] *Information for Law Enforcement Authorities*, META, https://about.meta.com/actions/safety/ audiences/law/guidelines/ (last visited May 14, 2024).

[255] Alfred Ng, *'A Uniquely Dangerous Tool': How Google's Data Can Help States Track Abortions*, POLITICO (July 18, 2022, 4:30 AM), https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906.

[256] Matthew Guariglia, *Geofence Warrants and Reverse Keyword Warrants are So Invasive, Even Big Tech Wants to Ban Them,* ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (May 13, 2022), https://www.eff.org/deeplinks/2022/05/geofence-warrants-and-reverse-keyword-warrants-are-so-invasive-even-big-tech-wants.

[257] Nate Raymond, *Firm Settles Massachusetts Probe over Anti-Abortion Ads Sent to Phones*, REUTERS (Apr. 4, 2017, 10:23 AM), https://www.reuters.com/article/us-massachusetts-abortion/firm-settles-massachusetts-probe-over-anti-abortion-ads-sent-to-phones-idUSKBN1761PX.

[258] *Id.*

[259] *Id.*

advertising firm agreed to discontinue its use of geofencing at or near Massachusetts healthcare facilities.[260]

Geofencing is already controversial in its existing form, but in this new era of abortion after *Dobbs*, geofence warrants will become invaluable tools in criminal and civil cases.[261] The information obtained through geofence warrants gives law enforcement the ability to reverse locate any individual who may have visited an abortion clinic. The nature of the information being sought need not be particularized—investigators simply circle an area on a map and compel a company to produce information identifying every device that entered the identified area during a given time.[262]

The constitutionality of the use of geofence warrants has already been the subject of much litigation. Civil rights groups like the ACLU have been active in their belief that geofence warrants are an unconstitutional practice that must be enjoined from use.[263] Notably, in 2018 the United States Supreme Court evaluated a similar issue concerning the use of reverse warrants to obtain cell phone tower information in *Carpenter v. United States*.[264] In *Carpenter*, law enforcement officers gathered cell-site location information ("CSLI") from a mobile phone provider that included the geographic location of cell phone users at any given time, without a probable cause warrant.[265] Officers were ultimately seeking records that would reveal the location of the defendant's cell phone whenever it made or received phone calls.[266]

For the first time, the court confronted questions about how substantial advancements in location technology impact a person's expectation of privacy. The court acknowledged that cell phone location information is "detailed, encyclopedic, and effortlessly compiled," and that wireless carriers have an interest in monitoring subscribers' location data in order to observe things like service performance and identify cell signal "dead zones."[267] Given the "unique nature of cell phone location records", the court held an individual "maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[268] The court, however, left undecided the issue of whether law enforcement seeking a "tower dump," where

---

[260] *Id.*
[261] *See* Tony Webster, *How Did the Police Know You Were Near a Crime Scene? Google Told Them,* MPR NEWS (Feb. 7, 2019, 3:10 PM), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants.
[262] GUARIGLIA, *supra* note 256.
[263] Nathan Freed Wessler, *The Supreme Court's Most Consequential Ruling for Privacy in the Digital Age, One Year In,* ACLU (June 18, 2019), https://www.aclu.org/news/privacy-technology/supreme-courts-most-consequential-ruling-privacy-digital.
[264] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[265] *Id.* at 2210.
[266] *Id.* at 2214.
[267] *Id.* at 2211-12, 2216.
[268] *Id.* at 2217.

information from any devices that connected to particular cell sites during particular times, would require a search warrant under the Fourth Amendment.[269] This "tower dump" of bulk data seems functionally similar to the types of data that would be gathered through geofencing, or location trackers on mobile devices from companies like Google or Facebook. Still, as a result of *Carpenter,* law enforcement must obtain a warrant in order to gain access to an identified individual's sensitive cellphone location data.[270]

Websites like Google are indispensable in modern times. Just as the court recognized in *Carpenter*, owning and carrying a cell phone is not truly voluntary anymore, because the services they provide are such "pervasive and insistent part[s] of daily life" that not carrying one would render an individual unable to participate in modern society.[271] The ruling in *Carpenter* was specific just to the facts of that case, and did not offer a wide sweeping application for all future third-party data related searches; yet, it shines a light on the third-party doctrine's incompatibility with the modern digital age.[272] Justice Sonia Sotomayor is similarly of the belief that the court will soon need to reconsider the principle that an individual has no expectation of privacy in information voluntarily given to third parties.[273] Future cases invoking the third-party doctrine will no doubt be closely watched by data privacy experts eager to see whether or how the court might expand its reasoning in *Carpenter* to the larger digital information landscape.

CONCLUSION

As the above demonstrates, there is now more than ever an overwhelming need in this country for comprehensive federal data privacy legislation. This need is even more striking after the events following the Supreme Court's opinion in *Dobbs*. For fifty years, abortion was a constitutional right nationwide—now, almost half of states have made it illegal. In a world where so much of daily life is spent engaged on the internet, abortion-related prosecutions and civil cases will almost certainly be sustained by digital evidence like web browser activity, internet search histories, location tracking, online shopping receipts, social media posts, text

[269] *Id.* at 2220.
[270] *Carpenter*, 138 S. Ct. at 2221.
[271] *Id.* at 2220 (citing Riley v. California, 573 U.S. 373, 385 (2014)).
[272] Ayoub & Goitein, *supra* note 238 ("The Supreme Court presumably will clarify *Carpenter*'s applicability in due time, but for now, government agencies are relying heavily on data purchases to sidestep the Fourth Amendment's central safeguard against abusive policing: the requirement that police obtain a warrant from a judge before invading a reasonable expectation of privacy.").
[273] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

and internet messages, and more. The most intimate details of someone's life—their reproductive healthcare decisions—will be on full display.

Up until now, online data privacy has largely been an individual's own responsibility to achieve, while private sector companies have had carte blanche to dictate how their data operations are conducted. While some states have taken steps to secure data privacy, it has resulted in an underwhelming patchwork of state laws that miss the mark. Existing federal laws similarly are incapable of meeting the moment. Now is the time for immediate action by the federal government to address these extant privacy concerns through robust legislation and agency action, and massive efforts to educate the public about maintaining privacy while using the internet and personal electronics.[274] Even those who disagree about abortion would likely agree on at least one thing: that the unmitigated mass collection, exploitation and profit off of our personal information is intolerable.

Lawmakers, defend our data.

[274] *See* Chris D. Linebaugh, Cong. Rsch. Serv., LSB10786, Abortion, Data Privacy, and Law Enforcement Access: A Legal Overview (2022); *See also Keep Your Abortion Private & Secure*, Digital Defense Fund, https://digitaldefensefund.org/ddf-guides/abortion-privacy/ (last visited May 14, 2024) (digital privacy tip sheet).