DIGITAL PRIVACY FOR REPRODUCTIVE CHOICE IN THE POST-*ROE* ERA

AZIZ Z. HUQ† AND REBECCA WEXLER‡

The overruling of Roe v. Wade *has unleashed a torrent of regulatory and punitive activity restricting previously lawful reproductive options. But the turn to the expansive criminal law and new schemes of civil liability creates novel concerns, quite distinct from the pre-*Roe *landscape a half-century ago. Reproductive choice, and its nemesis, turn upon information. For pregnant people, deciding on a choice of medical care entails a search for advice and services. Information is at a premium for them. Meanwhile, efforts to regulate abortion began with clinic closings. But they will quickly extend to civil actions and criminal indictments of patients, providers, and those who facilitate abortions. Like the pregnant themselves, criminal and civil enforcers depend on information. And in the contemporary context, the informational landscape, and hence access to counseling and services such as medication abortion, is largely mediated through digital forms of communication. In an era when most people use search engines or social media to access information, the digital architecture and data retention policies of those platforms will determine not only whether the pregnant can access medically accurate advice but also whether the act of seeking health information places them in legal peril.*

This Article offers an in-depth analysis of the core legal issues concerning abortion-related digital privacy after the end of Roe*. It demonstrates first that digital privacy for pregnant persons in the United States has suddenly become a tremendously fraught and complex question. It then maps the treacherous social, legal, and economic terrain upon which firms, individuals, and states will make privacy-related decisions. Building on this political economy, we develop a set of moral and economic arguments to the effect that digital firms should maximize digital privacy for pregnant persons within the scope of the law and should actively resist states' efforts to conscript them into a war on reproductive choice. We then lay out precise, tangible steps that firms should take to enact this active resistance. We explore here in particular a range of powerful yet legal options for firms to refuse cooperation with restriction-focused criminal and civil investigations. Finally, we present an original, concrete and immediately actionable proposal for federal and state legislative intervention: a statutory evidentiary privilege to shield abortion-relevant data from warrants, subpoenas, court orders, and judicial proceedings aimed at limiting the availability of reproductive care.*

† Frank and Bernice Greenberg Professor of Law, University of Chicago Law School, supported by the Frank J. Cicero fund.

‡ Assistant Professor of Law, University of California, Berkeley, School of Law. Thanks to Andrew Bradt, Khiara Bridges, Brandon Garrett, Anya Prince, and Natalie Ram for helpful comments on earlier drafts; to Summer Elliot, Izzy Simon, Maggie Wells, and Daniela Wertheimer for research assistance; and to Nicole Mo, Mariela Mannion, Deborah Leffell, Deven Kirschenbaum, and other editors of the *New York University Law Review* for excellent editorial feedback and careful work.

Introduction

When the Supreme Court overruled *Roe v. Wade*,[1] and eliminated the constitutional right to abortion,[2] the six Justices joining the majority opinion unleashed an explosion of regulatory and punitive activity by states bent on restricting the range of lawful reproductive options. The majority in *Dobbs v. Jackson Women's Health Organization* claimed that they anticipated that reproductive choice would henceforth be "resolved like most important questions in our democracy: by citizens trying to persuade one another and then voting."[3] Immediately on the ground, though, it was not so much deliberation and voting that prevailed as it was the coercive apparatus of criminal and civil enforcement. On the day *Dobbs* was handed down, thirteen states saw the operation of trigger laws that purported to reintroduce criminal prohibitions on abortion provision.[4] In one of these "restrictionist"[5] states, Texas, a group of legislators not only targeted in-state facilities but also threatened the partners of national law firms with criminal charges for their employee health plans.[6] This speedy turn to an expansive and minatory criminal law was no surprise. Indeed, the *Dobbs* Court implicitly invited the immediate and aggressive criminalization of medical care by using the negatively-freighted term "abortionist," rather than "providers" or "clinicians," throughout the majority opinion.[7]

---

[1] 410 U.S. 113 (1973).

[2] Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2284 (2022) ("The Constitution does not prohibit the citizens of each State from regulating or prohibiting abortion.").

[3] *Id.* at 2243.

[4] Elizabeth Nash & Isabel Guarnieri, *13 States Have Abortion Trigger Bans—Here's What Happens When Roe Is Overturned*, Guttmacher Inst. (June 6, 2022), https://www.guttmacher.org/article/2022/06/13-states-have-abortion-trigger-bans-heres-what-happens-when-roe-overturned [https://perma.cc/B962-J3UA].

[5] We use the term "restrictionist" to characterize states that regulate abortion in ways that would have been impermissible prior to *Dobbs*.

[6] Debra Cassens Weiss, *Texas GOP Warns that Sidley Partners Could Be Prosecuted if the Firm Pays Abortion Travel Costs*, ABA J. (July 11, 2022), https://www.abajournal.com/news/article/texas-gop-group-warns-sidley-partners-could-be-prosecuted-if-the-firm-pays-abortion-travel-costs [https://perma.cc/HHH6-PNHF]. A Republican appointee to the federal Equal Employment Opportunity Commission has also begun discrimination investigations into companies that facilitate their employees' travel to obtain reproductive care. J. Edward Moreno, *EEOC Official Quietly Targets Companies Over Abortion Travel*, Bloomberg L. (Nov. 14, 2022, 5:15 AM), https://news.bloomberglaw.com/daily-labor-report/eeoc-official-quietly-targets-companies-over-abortion-travel-20 [https://perma.cc/ARV3-ZNVS].

[7] *Dobbs*, 142 S. Ct. at 2250, 2254; *see also Doctors Weren't Considered in Dobbs, but Now They're on Abortion's Legal Front Lines*, NPR (July 3, 2022), https://www.npr.org/transcripts/1109483662 [https://perma.cc/DT8V-5QZG] (noting the American College of

By the beginning of July 2022—merely a week after *Dobbs*—eight of those thirteen states with extant criminal prohibitions on abortion had kicked these punitive laws into force.[8] Several of these legal regimes, including Kentucky's, South Dakota's, and Louisiana's, contain exceptions for when the mother's life is at risk but not for when their health is seriously imperiled; nor do they carve out cases of rape or incest.[9] Under such laws, providers can be charged with "some class of felony, with punishments that include fines, prison time and revocation of medical licenses."[10] Louisiana's statute, for example, imposes sentences up to two years, or fines of up to $1,000;[11] Idaho's allows sentences between two and five years for people who perform abortions, as well as professional discipline including the suspension or termination of medical licenses for medical providers.[12] Texas's Attorney General, further, sued to enjoin a federal mandate to provide abortion services under emergency conditions—in effect, demanding that the state's prohibition on abortion override not just a person's right to choice but also the right to life.[13] Beyond these criminal law instruments, states such as Texas, Idaho, and Oklahoma have, within the last two years, enacted statutes permitting private citizens to seek civil penalties against abortion providers and others.[14]

Obstetricians and Gynecologists' criticisms of Justice Alito's choice of words as "[i]nflammatory" and "inaccurate").

[8] Ava Sasani, *What's Happening in the States? Here's the Latest on Which Abortion Laws Are in Effect and Which Are Blocked*, N.Y. TIMES (July 1, 2022), https://www.nytimes.com/2022/07/01/us/abortion-bans-laws-blocked-us-states.html [https://perma.cc/4NR3-2B6S]. For more updated data, see *Tracking the States Where Abortion Is Now Banned*, N.Y. TIMES, https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html [https://perma.cc/8J77-6KTG] (reporting thirteen states with full bans and one state, Georgia, with a ban starting six weeks after conception).

[9] *See* Nash & Guarnieri, *supra* note 4.

[10] Safia Samee Ali, *Prosecutors in States Where Abortion Is Now Illegal Could Begin Building Criminal Cases Against Providers*, NBC NEWS (June 24, 2022, 7:17 PM), https://www.nbcnews.com/news/us-news/prosecutors-states-abortion-now-illegal-begin-prosecute-abortion-provi-rcna35268 [https://perma.cc/5EKJ-GLF7].

[11] LA. STAT. ANN. § 40:1061.29 (2015).

[12] IDAHO CODE ANN. § 18-605 (West 2022); *see also* Nash & Guarnieri, *supra* note 4.

[13] *See* Christine Vestal, *Some Abortion Bans Put Patients, Doctors at Risk in Emergencies*, PEW TRUSTS: STATELINE (Sept. 1, 2022), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/09/01/some-abortion-bans-put-patients-doctors-at-risk-in-emergencies [https://perma.cc/PZE3-GD8Q].

[14] On Texas's law, see Texas Heartbeat Act, S.B.8, 87th Leg., Reg. Sess. (Tex. 2021) (codified at TEX. HEALTH & SAFETY CODE ANN. § 171.208(a)(1) & (2) (West 2021)) (allowing any private party to bring a suit for damages of no less than $10,000 or injunctive relief against a person who "performs or induces" a covered abortion or knowingly "aids or abets the performance or inducement of an abortion," whether or not the person knows abortions have been banned). On Oklahoma's law, see Jessica Glenza, *Oklahoma Republican-Led Legislature Passes Nation's Strictest Abortion Ban*, THE GUARDIAN (May 19, 2022, 4:20 PM), https://www.theguardian.com/us-news/2022/may/19/oklahoma-

Criminal law enforcement efforts will therefore be supplemented by private legal actions and private investigative efforts.

There is, to be clear, little new in the deployment of the criminal law and its violent adjuncts as instruments to regulate intimate "morals." The practice goes back to the beginning of the Republic.[15] The historian William Novak has described a "transformation in attitudes toward morality around 1776 . . . in the direction of increased rather than decreased public attention . . . [and] one of the most concerted and energetic moral reform movements in American history."[16] Writing in 1904, law professor Ernst Freund of the University of Chicago merely echoed the putative wisdom of his day when he explained that the "cultivation of moral, intellectual and aesthetic forces and interests which advance civilization and benefit the community . . . cannot be a matter of indifference to the state."[17] The criminal law was used to "reinforce family law's substantive restrictions. Family law says what marriage is, and criminal law . . . criminaliz[ed] behavior, and actors, ineligible for marriage."[18] Pregnancy, as a result, has long been in prosecutors' crosshairs. A 2013 scholarly study identified 413 cases arising between 1973 and 2005 in which the fact of pregnancy was a necessary predicate for an attempted or successful criminal action (despite *Roe*).[19] A non-profit conducting a follow-on study found approximately 1,331 additional instances between 2006 and 2020 in which pregnancy was a predicate

---

abortion-ban-strictest [https://perma.cc/7KFA-GNNG]. On Idaho's measure, see Sarah McCammon, *Idaho Prepares to Ban Most Abortions in the State as Governor Signs Texas-Style Law*, NPR (Mar. 24, 2022, 11:05 AM), https://www.npr.org/2022/03/23/1087202877/idaho-prepares-to-ban-most-abortions-in-the-state-as-governor-signs-texas-style [https://perma.cc/7BYS-ZCF8]. For a history of these laws, see Aziz Z. Huq, *The Private Suppression of Constitutional Rights*, 101 TEX. L. REV. (forthcoming May 2023) (manuscript at 11–37), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4072800 [https://perma.cc/ZD76-YH99].

[15] *See* JOHN D'EMILIO & ESTELLE B. FREEDMAN, INTIMATE MATTERS: A HISTORY OF SEXUALITY IN AMERICA 15–32 (1988); *accord* LAWRENCE M. FRIEDMAN, CRIME AND PUNISHMENT IN AMERICAN HISTORY 127–32 (1993) (detailing history of moral crimes).

[16] WILLIAM J. NOVAK, THE PEOPLE'S WELFARE: LAW AND REGULATION IN NINETEENTH-CENTURY AMERICA 152 (1996).

[17] ERNST FREUND, THE POLICE POWER: PUBLIC POLICY AND CONSTITUTIONAL RIGHTS 9 (1904).

[18] Melissa Murray, *Strange Bedfellows: Criminal Law, Family Law, and the Legal Construction of Intimate Life*, 94 IOWA L. REV. 1253, 1268 (2009). For a detailed history of the recourse to criminal law to enforce men's family support obligations, see Elizabeth D. Katz, *Criminal Law in a Civil Guise: The Evolution of Family Courts and Support Laws*, 86 U. CHI. L. REV. 1241, 1260–61 (2019).

[19] Lynn M. Paltrow & Jeanne Flavin, *Arrests of and Forced Interventions on Pregnant Women in the United States, 1973–2005: Implications for Women's Legal Status and Public Health*, 38 J. HEALTH POL., POL'Y & L. 299, 299–300 (2013).

for criminal prosecution.[20] So it is no surprise that the criminal law—and in particular its use as an instrument of moral conformity—lurked closely in the background of the first Supreme Court disputes concerning the constitutional right to sexual privacy.[21]

Yet "morals regulation" using the criminal law circa 2023 poses new and quite different concerns from those of a century, or even a half-century, ago. Reproductive choice and its nemesis rest on information. For pregnant people, deciding on a choice of medical care entails a search for advice and services. Meanwhile, efforts to regulate abortion begin with clinic closings but quickly will fan out into civil actions and criminal indictments of patients, providers, and those who facilitate abortions.[22] Like the pregnant themselves, restrictionist enforcers depend upon information.

In the contemporary context, both the search for support of reproductive choice and efforts to suppress it play out in a digital landscape. Ours is an era in which most people use search engines or social media to access information. So the digital architecture and data retention policies of those platforms will determine not only whether the pregnant can access medically accurate advice but also whether the mere act of doing so places them in legal peril by leaving a discoverable digital trace. Access to counseling and services such as medication abortion are now increasingly digitized and online. A medication abortion involves the use of drugs such as mifepristone and misoprostol, both currently approved by the Food and Drug Administration (FDA), up through seventy days of pregnancy.[23] During the COVID-19 pandemic, the FDA relaxed in-person dispensing requirements to allow prescriptions based on medical history

[20] *Arrests and Prosecutions of Pregnant Women, 1973-2020*, PREGNANCY JUST. (Sept. 18, 2021), https://www.pregnancyjusticeus.org/arrests-and-prosecutions-of-pregnant-women-1973-2020 [https://perma.cc/FB7S-NRBV].

[21] *See* Melissa Murray, Essay, Griswold*'s Criminal Law*, 47 CONN. L. REV. 1045, 1061 (2015). In a subsequent piece, Murray identifies three forces driving increasing deregulation of sexual morality: "(1) the liberalization of laws criminalizing private, consensual adult sex; (2) the emerging sensibility that the state should not use the criminal law to express moral judgments about private, consensual, sexual behavior; . . . (3) the emergence—and expansion—of constitutional protection for private, consensual adult sex, whether marital or not." Melissa Murray, Essay, *Rights and Regulation: The Evolution of Sexual Regulation*, 116 COLUM. L. REV. 573, 581–82 (2016) (footnotes and citations omitted).

[22] *See supra* notes 8–13 and accompanying text (discussing the spate of laws imposing criminal and civil penalties for abortion).

[23] Ushma D. Upadhyay, Elizabeth G. Raymond, Leah R. Koenig, Leah Coplon, Marji Gold, Bliss Kaneshiro, Christy M. Borass & Beverly Winikoff, *Outcomes and Safety of History-Based Screening for Medication Abortion: A Retrospective Multicenter Cohort Study*, 182 JAMA INTERNAL MED. 482, 483 (2022).

alone, opening the door to online and telemedicine prescriptions.[24] A study of 3,779 patients who had undergone medical abortions based solely on medical history reported complications in only 0.54% of cases.[25] An additional study, focused on medical abortion by telemedicine, found no statistically significant differences in health risks or complications between in-person and telemedicine medication abortion groups.[26] Medical providers in *Dobbs*'s wake found themselves "pushing the envelope" to meet a surging demand for such medication abortion.[27] The availability of digitally mediated advice, medication, and services lowers the costs of becoming educated and accessing care. But it also creates new angles of exposure to criminal and civil liability.[28]

Today, unlike in 1973, prosecutors and civil litigants searching for the formerly pregnant or for those potentially seeking to terminate a pregnancy can mine a vast universe of digital data. This is not just a result of accessing search engines or provider websites. Abortion-relevant data is also generated by cellphones, portable fitness devices, vehicles, cameras, interactions with employers and medical personnel, and other uses of technology. Many of these digital traces can be used not just to undo access to medical care but also to undermine what Danielle Keats Citron, in an important article, calls "sexual privacy—the social norms (behaviors, expectations, and decisions) that govern access to, and information about, individuals' intimate lives."[29]

This efflorescence of digital data poses well-recognized challenges for Fourth Amendment privacy in general.[30] The implications for a

---

[24] *Id.*

[25] *Id.*

[26] Julia E. Kohn, Jennifer L. Snow, Hannah R. Simons, Jane W. Seymour, Terri-Ann Thompson & Daniel Goldman, *Medication Abortion Provided Through Telemedicine in Four US States*, 134 OBSTETRICS & GYNECOLOGY 343, 343, 348 (2019).

[27] Pam Belluck, *Abortion Pill Providers Experiment With Ways to Broaden Access*, N.Y. TIMES (Sept. 3, 2022, 11:19 AM), https://www.nytimes.com/2022/09/03/health/abortion-pill-access-roe-v-wade.html [https://perma.cc/2ZNC-VF7L].

[28] *See, e.g.*, Melissa Quinn, *Justice Department's Warning to States Over Abortion Pill Bans Points to Legal Fight Ahead*, CBS NEWS (July 6, 2022, 8:42 AM), https://www.cbsnews.com/news/medication-abortion-mifepristone-roe-v-wade-supreme-court-justice-department [https://perma.cc/AR5S-H8UU] (warning that recent Justice Department guidance telling states not to ban mifepristone may mark medication abortion as "the next front in the fight to preserve abortion rights").

[29] Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1874 (2019).

[30] *See, e.g.*, Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 554 (2017) (discussing characteristics of digital data that "undermine the distinctions that mark Fourth Amendment doctrine"); Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 566–603 (2017) (applying existing Fourth Amendment doctrine to data trails recorded by smart devices); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1320–35 (2012) (describing how traditional Fourth Amendment doctrine, coupled with

post-*Roe* world of roving restrictionist Javerts, public and private, have yet to be understood in full. Even in the immediate twilight of constitutional reproductive privacy rights, and before the machinery of state power has cranked up, it is plain that concerns both for reproductive choice and for privacy more generally are serious. In 2015, for example, an Indiana woman was convicted on felony charges related to her fetus's death on the basis of text messages related to abortion medications she sent to a friend.[31] In 2017, a woman was indicted for second-degree murder after a stillbirth, with the prosecution pointing to mentions of misoprostol in her internet search history.[32] And in August 2022, Nebraska police reportedly used a warrant to acquire digital data from Facebook in order to indict a forty-one-year-old woman on a felony charge related to her daughter's decision to seek an abortion.[33] We very much doubt that this will be the last such instance in which digital data is used to further restrictionist ends after *Dobbs*.

At the same time, it seems very unlikely that the Supreme Court today will impose any significant privacy-related barriers to such prosecutions. This creates another profound difference between the pre-*Roe* and the post-*Dobbs* landscape. Seventy-odd years ago, "concerns about homosexuality, and about the policing of homosexuality" prompted the Court to strengthen criminal procedure rights.[34] Now, however, it seems far more probable that the Roberts Court will do away with established criminal procedure entitlements in its zeal to facilitate the hunt for "abortionists."[35]

The scope and operation of abortion-related digital privacy is not just a function of decisions by restrictionist prosecutors and civil liti-

---

recent technological advances, could significantly expand government surveillance power); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084–86 (2002); *see also* SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA 221–63 (2018) (charting the emergence of privacy concerns about records in the 1960s).

31 Ali, *supra* note 10.

32 *Id.*

33 Martin Kaste, *Nebraska Cops Used Facebook Messages to Investigate an Alleged Illegal Abortion*, NPR (Aug. 12, 2022, 2:49 PM), https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion [https://perma.cc/H2M2-B5D5].

34 David Alan Sklansky, *"One Train May Hide Another":* Katz*, Stonewall, and the Secret Subtext of Criminal Procedure*, 41 U.C. DAVIS L. REV. 875, 877–78 (2008).

35 This morally loaded term of opprobrium features prominently in *Dobbs v. Jackson Women's Health Org.*, 142 S. Ct. 2228, 2250, 2254 (2022). For an example of the potential path of the Court in respect to the important question of habeas remedies, see Justice Gorsuch's concurrence, joined by Justice Thomas in *Edwards v. Vannoy*, 141 S. Ct. 1547, 1566 (2021) (Gorsuch, J., concurring) (arguing that the Court should not inquire into the process preceding a final state court conviction).

gants. Other actors play a decisive role. Opportunities to protect digital privacy will turn on how social media platforms and other commercial actors who engage with data respond to *Dobbs*; what forms of digital empowerment these firms make available to individual pregnant patients and how the patients behave; and whether state and federal lawmakers protective of safe reproductive care act through legislation or regulation to advance digital privacy. The regulatory terrain, in short, is highly complex. It is not just a function of the formal law on the books. It will crystallize out of a combination of individual actions and commercial decisionmaking—especially in respect to the architecture of digital transactions and the wider data-related economy—as well as formal legal rules.

This Article offers an in-depth accounting of abortion-related digital privacy after *Dobbs*. Our aim is to build on the growing recognition that digital privacy for pregnant persons in the United States has suddenly become a tremendously fraught and complex question. We first aim to elucidate, as a positive matter, the complex social, legal, and economic terrain upon which firms, individuals, and states will make privacy-related decisions. Beyond this political economy, we develop a moral and economic argument that digital firms should maximize digital privacy for pregnant persons within the scope of the law and should actively resist restrictionist states' efforts to instrumentalize them into their war on reproductive choice.

We then lay out precise, tangible steps that firms should take to enact this active resistance, explaining a range of powerful yet legal options for firms to refuse cooperation with restrictionist criminal and civil investigations.

Finally, we present an original, concrete, and immediately actionable proposal for legislative intervention at either the state or the federal level: the enactment of statutory evidentiary privileges that shield abortion-relevant data from restrictionist warrants, subpoenas, court orders, and judicial proceedings. Such a privilege was first proposed publicly (by one of us) in congressional testimony on July 19, 2022.[36] We demonstrate that the privilege could also be adopted at the state level.

Our work here builds on and extends a published literature. One pre-*Dobbs* law review article by Cynthia Conti-Cook discusses exten-

[36] *See* H. Comm. on the Judiciary, *Digital Dragnets: Examining the Government's Access to Your Personal Data*, YOUTUBE, at 02:30:00 (July 19, 2022), https://www.youtube.com/watch?v=F27nOcsenRY&ab_channel=HouseCommitteeontheJudiciary [https://perma.cc/WXQ2-M49S]; *Digital Dragnets: Examining the Government's Access to Your Personal Data: Hearing Before the H. Comm. on the Judiciary*, 117th Cong. (2022) (statement of Rebecca Wexler).

sively the use of digital evidence in pregnancy-related prosecutions.[37] Conti-Cook takes a historical lens on medical surveillance before identifying some angles from which patients are digitally exposed with respect to abortion restrictions and considering how "social justice movements" and criminal defenders could respond.[38]

A post-*Dobbs* scholarly conversation more expansively interrogates the relationship between digital privacy and access to abortion. Multiple scholars have recognized that digital surveillance infrastructure can be mobilized for restrictionist investigations, and that poor, underserved communities of color are likely to be disproportionately targeted.[39] Anya Prince and Allyson Haynes Stuart advocate for new federal data privacy legislation to protect access to abortion and other reproductive health services.[40] Leah Fowler and Michael Ulrich, in contrast, express skepticism that Congress can effectively pass and implement federal data privacy legislation, and worry that any legislation that does pass will include exceptions that permit law enforcement to access the protected data and thus do little to prevent restrictionist prosecutions.[41] Additional policy reports, published by

---

[37] *See generally* Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV. 1 (2020).

[38] *Id.* at 22–58, 66, 70–71 (briefly discussing legal responses, focusing on the role of criminal defenders); Michele Estrin Gilman, *Feminism, Privacy and Law in Cyberspace*, *in* OXFORD HANDBOOK OF FEMINISM AND LAW IN THE U.S. 6 (Deborah Brake et al. eds., 2021) (ebook) (briefly discussing antiabortion activists' use of digital technologies such as geofencing to target people seeking abortions).

[39] *See, e.g.*, Elizabeth E. Joh, *Dobbs Online: Digital Rights as Abortion Rights*, *in* FEMINIST CYBERLAW (Amanda Levendowski & Meg Leta Jones eds., forthcoming 2024) (manuscript at 3–5, 7–8), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210754 [https://perma.cc/D5ET-2NRL]; *see also*, Khiara M. Bridges, *Forward: Race in the Roberts Court*, 136 HARV. L. REV. 23, 42–55 (2022) (observing that Black people use abortion services at higher frequencies and will be disproportionately impacted by post-*Dobbs* abortion bans).

[40] Anya Prince advocates for a comprehensive federal data privacy law capacious enough "to truly protect reproductive health privacy," including protections from "companies collecting data, data brokers, and law enforcement access of data beyond warrants, such as informal requests or purchasing." Anya E.R. Prince, *Reproductive Health Surveillance*, 64 B.C. L. REV. (forthcoming 2023) (manuscript at 51–52), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4176557 [https://perma.cc/W64V-LJJF]. Prince emphasizes the benefits not only for abortion access but also for reproductive health privacy more generally. *Id.* at 36–40. Allyson Haynes Stuart also raises concern that *Dobbs*'s undermining of the constitutional right to privacy will erode protections against civil discovery of reproductive health and other personal information, including not only in antiabortion civil lawsuits but also in sexual harassment claims and claims alleging physical or mental injury. Allyson Haynes Stuart, *Privacy in Discovery After* Dobbs, 26 VA. J.L. & TECH. 4, 5–8, 31 (2023). Stuart advocates express codification of a privacy interest in civil discovery balancing tests, as well as more general legislation recognizing a right to informational privacy. *Id.* at 30–31.

[41] Leah R. Fowler & Michael R. Ulrich, *Femtechnodystopia*, 75 STAN. L. REV. (forthcoming 2023) (manuscript at 59–65), https://papers.ssrn.com/sol3/papers.cfm?

the Surveillance Technology Oversight Project and the Electronic Frontier Foundation, among others, look at a wide range of surveillance pathways and the choices confronting private actors.[42] Yet the brevity of these reports means that they only hint at the range and complexity of legal issues in the post-*Dobbs* digital landscape. The implications of our digital economy for both access to abortion services and the attendant risk of prosecution have also been intermittently glimpsed in media reports but have not received any sustained mapping.[43]

Each of those writings makes valuable points. We strive to build on their contributions, not duplicate them, by developing a more comprehensive yet transparent typology of relevant digital information flows; by more closely examining the role of private actors in the post-*Dobbs* world, and by offering a clearer explanation of the ensuing pro-privacy options for privacy-friendly firms and states. To our knowledge, for example, no prior work has detailed the extent to which firms can refuse cooperation with restrictionist law enforcement demands while remaining within the letter of the law. And no prior work has proposed enacting evidentiary privileges to shield abortion-relevant data from restrictionist enforcement efforts.

Our specific aims in this Article are threefold. First, we offer a positive account of how the architecture of digital information flows interacts with the hydraulics of reproductive choice and the strategies of its foes. By doing so, we clarify the ways in which structural choices made within the digital economy create opportunities for both reproductive choice's allies and its enemies. We underscore here in particular the bilateral character of the flow of information (to patients and

---

abstract_id=4099764 [https://perma.cc/9UDT-8LHY]. Fowler and Michael more generally argue that in a post-*Dobbs* era portending increased state restrictions on contraception, state intrusion into medical decisions surrounding birth, and more general state surveillance and control over those who may become pregnant, period and fertility tracking apps can provide greater autonomy over pregnancy while at the same time generating data that may end up "in the hands of nefarious actors or facilitate civil and criminal actions[.]" *Id.* at 27. They suggest ways that app developers can minimize privacy risks by limiting data collection and adopting design choices such as end-to-end encryption, *id.* at 69–71, and identify a number of ways that users can engage in digital self-defense, *id.* at 71–75.

[42] *See, e.g.*, Albert Fox Cahn & Eleni Manis, *Pregnancy Panopticon: Abortion Surveillance After* Roe, SURVEILLANCE TECH. OVERSIGHT PROJECT 6–7, 9–13 (May 24, 2022), https://www.stopspying.org/pregnancy-panopticon [https://perma.cc/D9PY-5YNT]; Corynne McSherry & Katharine Trendacosta, *What Companies Can Do Now to Protect Digital Rights in a Post-*Roe *World*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (May 10, 2022), https://www.eff.org/deeplinks/2022/05/what-companies-can-do-now-protect-digital-rights-post-roe-world [https://perma.cc/RDP5-9259].

[43] *See, e.g.*, Kaste, *supra* note 33 (describing the use of Facebook messages to prosecute a mother and daughter for violating abortion laws).

to their persecutors), which makes the digital domain an inconstant friend where reproductive choice is concerned. This map of the informational (or epistemic) landscape on which the new abortion wars will unroll does double duty as a guide for those concerned with their vulnerability to state supervision.

Second, we analyze the ethical, legal, and economic dilemmas faced by crucial sets of private actors: technology firms and their users. We show that search firms, social media, data brokers, and platforms—indeed any firm with a digital footprint falls into the scope of what we call a "digital" or a "technology" firm—will have to make fraught choices post-*Dobbs*. The modal response of tech firms to date has been to suggest they will firmly defend their employees' access to reproductive services, but not their users'.[44] This line is untenable. Worse for tech companies hoping to avoid taking a position, we demonstrate that private firms will not be able to use geographic boundaries to demarcate zones of compliance with law enforcement, as opposed to respect for reproductive choice. Neither patients nor restrictionist enforcement efforts will respect state lines. Digital firms, therefore, will inevitably be forced to choose whether to cooperate with restrictionist efforts turning on persons or data located outside the geographical bounds of states that limit abortion. Similarly, data gathered in restrictionist states can reveal activities by providers and pregnant persons within states where abortion is broadly lawful. The risk of such exposure is likely to have a chilling effect. The comprehensive blurring of geographic lines also means that digital firms must take sides: There is no neutral ground.

In light of these dynamics, we canvas the ethical and economic arguments for minimizing, within legal bounds, the extent to which technology firms' digital architectures and prior actions expose their users to abortion-related investigation and prosecution. We conclude that there are powerful reasons for some (if not all) companies to maximize privacy by design—and even at the margins take on some risk of law-related costs in the defense of reproductive choice—based on their own narrowly conceived commercial interests.

---

[44] And indeed, not all workers. *See* Caitlin Harrington, *Tech Companies Will Cover Abortion Travel, but Not for All Workers*, WIRED (July 7, 2022, 7:00 AM), https://www.wired.com/story/tech-companies-abortion-travel [https://perma.cc/9FUL-DKMJ]. Further, given the speed at which such policies were rolled out, it is reasonable to ask whether they will be durable. *See* Jacob Kastrenakes, *Why Big Tech Companies Are So Quiet on Abortion Rights*, THE VERGE (June 30, 2022, 1:56 PM), https://www.theverge.com/2022/6/30/23189810/abortion-rights-activism-big-tech-employees [https://perma.cc/QKP6-G2JW] (reporting "quick, makeshift policies aligning these companies with the right to choose and granting benefits that supported that stance").

Finally, we shift into a prescriptive gear to ask what can be done—by firms and individuals and even pro-choice states—to maximize digital privacy in relation to reproductive choice.[45] To this end, we offer a taxonomy of what we dub "battlefields" in the coming abortion wars. These battlefields are four distinct "quarters" of the digital world in which the abortion wars might unfold: (1) technology firms' decisions to collect and retain data; (2) technology firms' responses to regulators' demands for information; (3) technological infrastructure that empowers individual users to access information privately and securely; and (4) state and federal data privacy and evidentiary privilege regulation or legislation. These four battlefields, for patients and regulators alike, act as substitutes in part and complements in part. Clarifying their interrelationship helps focus on where and how reproductive choice can best be enabled—or repressed. What ensues from this analysis is a manifesto for digital privacy to enable reproductive choice.

Lest there be any doubt about the perspective from which we write, we should clarify up front our normative priors. We approach the analysis on the assumption that *Dobbs* was incorrectly decided as a matter of law and as a moral matter. A view of the fundamental rights to life and liberty under the Fourteenth Amendment should account for all Americans' experience. It should not be insensitive to the radical political exclusion women have experienced through much American history. So understood, historical inquiry of the sort supposedly deployed in *Dobbs* would quickly reveal the centrality of reproductive choice to the felt experience of liberty and life. We are further persuaded by the moral case in favor of abortion developed by philosophers such as Judith Jarvis Thompson and Richard Hare.[46]

Unlike the *Dobbs* Court, moreover, we are alive to the relation between restrictionist regulation and the marginalization and disempowerment of women as a class even as we are aware of the way in

---

[45] We do not address here the federal administrative state, including the FDA and other agencies. Presumably, the latter's posture will change radically depending on which party controls the White House. It would be peculiar to plot out choice-enabling regulatory strategies on the (false) assumption that federal policy won't change.

[46] Judith Jarvis Thomson, *A Defense of Abortion*, 1 PHIL. & PUB. AFFS. 47, 48–49 (1971) (stipulating the personhood of the fetus and developing a counterargument to claims against abortion based on the pregnant person's autonomy interests). For an illuminating defense of abortion under the "Christian golden rule," see R.M. Hare, *Abortion and the Golden Rule*, 4 PHIL. & PUB. AFFS. 201, 221 (1975). On the dearth of religious opposition to abortion as a historical matter until the twentieth century, see Garry Willis, *The Bishops Are Wrong About Biden—and Abortion*, N.Y. TIMES (June 27, 2021), https://www.nytimes.com/2021/06/27/opinion/biden-bishops-communion-abortion.html [https://perma.cc/9JJH-LA53] (exploring the absence of opposition to abortion in historical Christianity).

which abortion sweeps in those who do not identify as women while experiencing pregnancy.[47]

Although we disagree sharply with *Dobbs* on both legal and moral grounds, we nevertheless stipulate its outcome as a matter of positive (but unjust and incorrect) law for the purposes of analysis here. Our approach is, at the same time, sensitive to the powerful liberty, anti-domination, and equality interests at stake when reproductive choice is curtailed. The Court's failure to recognize or honor those interests is hardly warrant for the rest of us to do the same. Nor is the bare fact of criminalization enough to squelch the powerful moral and medical interests that the pregnant have in accessing information and care. American history is full of instances in which state-level criminalization and pendent investigative powers have been used for morally bankrupt ends such as the enforcement of chattel slavery before the Civil War[48] or its recreation through "Black Codes" and convict leasing laws in the late eighteenth century.[49]

Our argument in the balance of the paper proceeds as follows. Part I crisply maps the bilateral economy of digital data flows—to patients and to prosecutors—that works as terrain in the new abortion wars. We draw attention here in particular to epistemic dynamics that, to date, have been understudied or ignored. Part II turns to the ethical and economic choices of technology firms straddling this landscape. We ask here both what would be ethical, and what would be efficient (i.e., wealth-maximizing), for different firms to do. Part III then offers a taxonomy of digital battlefields. It points the way toward complementary choices by private firms, individuals, and choice-favoring legislatures that would expand access to reproductive care without the risk of state coercion.

I
The Epistemic Economy of Abortion and Its Regulation

This Part sets out the epistemic economy of post-*Dobbs* conflict over abortion. Its core thesis is that this economy is made up of two

---

[47] While centering the historical role of misogynistic ideas, we also acknowledge the spillovers that abortion has on those close to the regulated person. The main text, in other words, should not be understood as a repudiation of the moral complexity of how abortion bans affect real families.

[48] *See* Sally E. Hadden, Slave Patrols: Law and Violence in Virginia and the Carolinas 114 (2001).

[49] *See* Rebecca M. McLennan, The Crisis of Imprisonment: Protest, Politics, and the Making of the American Penal State, 1776–1941, at 85–86 (2008) (exploring ways in which the exception in the Thirteenth Amendment was exploited).

interlocking parts. On one side is the search for information by pregnant persons in relation to reproductive choice. On the other, the act of seeking and then acting upon this information cuts the grooves along which the investigative efforts of restrictionist actors largely run. This is because the former creates trails of data that can later be used to infer the fact of pregnancy and actions (even tentative or incomplete) toward the termination of a pregnancy.[50] This bilateral, or mirroring, dynamic arises because of the way in which digital activity leaves traces that allow a subsequent reconstruction of an actor's movements, decisions, and even (by inference) thoughts while online. In contrast, activity in the physical world is much less likely to leave behind traces that allow a subsequent actor to come along afterward and reconstruct earlier searches, communications, and acquisitions. The migration of activity from the physical world to the digital world therefore creates a mirroring—what is done at first can be mirrored and hence reconstructed later. This mirroring dynamic has no close precedent in the pre-*Roe* era.

We begin by exploring this mirroring relation between digital activity by potential patients and the investigative activity of those seeking to prevent abortions because it helps explain the potent strategies both for advancing and retarding reproductive privacy in an increasingly digitized context. We then briefly sketch the digital economy against which epistemic conflict over abortion arises. We outline the patient's search challenge, the ensuing restrictionist's challenge of drawing inferences from the ensuing data trails, and the strategies for epistemic access to restrictionist ends.

A. The Ecosystem of Digital Data

Conflict over abortion access occurs against the context of a new economic logic, often called "surveillance capitalism" or "informational capitalism," that is organized around the acquisition and exploitation of personal data.[51] Such data is produced, as most readers will know, as an unintended byproduct of access to internet search

---

[50] There is one important exception to this bilateral, or mirroring, dynamic that we set forth below arising from the power of machine-learning tools to leverage non-search activities to draw inferences about private facts.

[51] Aziz Z. Huq, *The Public Trust in Data*, 110 GEO. L.J. 333, 345 (2021) ("The collection of personal data as a collateral, often unwitting, side effect of platform use is central to the business model of other platforms."); *see also* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 1–2 (2019) (analyzing how legal institutions pervade, enable, and are influenced by the data-driven economy). The idea of surveillance capitalism is developed in SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 85 (2019) (arguing that data-based business models, which rely

tools, social media platforms and other communication apps, and web-based services to make purchases or access services via a smartphone or another wired device.[52] A great deal of data is created this way. There are approximately 307.2 million internet users in the United States, of which 282.48 million access the internet via mobile devices.[53] Personal data are also generated by one's physical movement through the world. Data are produced, for example, by location-tracking tools in cellphones, Fitbits, and other devices carried or worn on the body.[54] They are output by sensors built into smart vehicles.[55] Their production is also a consequence of a broader "Internet of things." This term is used to describe the way in which ordinary devices are armed with sensors and capable of transmitting data to central servers.[56] The result is an "exaflood" of data concerning individuals' physical states, movements, interests, and moods on a minute-by-minute basis.[57]

The personal data thereby created is increasingly commercially valuable because it can be analyzed to "infer and deduce the thoughts, feelings, intentions, and interests of individuals."[58] Such information is frequently monetized through the sale of digital advertising.[59] The

---

on the collection of personal data for the purpose of behavioral advertising, constitutes a new model of "surveillance capitalism").

[52] Omri Ben-Shahar, *Data Pollution*, 11 J. LEGAL ANALYSIS 104, 105 (2019) ("Digital platforms are learning who and where people are at any given time, what they did in the past and how they plan their future, what and who they like, and how their decisions could be influenced.").

[53] *Internet Usage in the United States—Statistics & Facts*, STATISTA (Oct. 18, 2022), https://www.statista.com/topics/2237/internet-usage-in-the-united-states [https://perma.cc/5SDX-K9ER].

[54] *See, e.g.*, Ben-Shahar, *supra* note 52, at 113 (discussing the uses of locational data generated by the Strava fitness app).

[55] Cade Metz, *How Driverless Cars See the World Around Them*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/how-driverless-cars-work.html [https://perma.cc/N9GQ-EXRN] (describing LIDAR, GPS, and other sensors built in to smart vehicles); *see also* Michael Mattioli, *Autonomy in the Age of Autonomous Vehicles*, 24 B.U. J. SCI. & TECH. L. 277, 283 (2018) (listing the "most common types of data captured by autonomous vehicles").

[56] Ferguson, *supra* note 30, at 548 ("From smartphones, fitness trackers, enchanted pill bottles, smart cars, and even smart refrigerators, these objects create extensive data trails revealing personal information, patterns, and activities."). For an excellent general introduction to the concept and its applications, see SAMUEL GREENGARD, THE INTERNET OF THINGS (2015).

[57] LUCIANO FLORIDI, INFORMATION: A VERY SHORT INTRODUCTION xxi (2010); *see also* CARL BENEDIKT FREY, THE TECHNOLOGY TRAP: CAPITAL, LABOR, AND POWER IN THE AGE OF AUTOMATION 303–04 (2019) (describing the scale of data produced by the internet); Jeff Desjardins, *How Much Data Is Generated Each Day?*, WORLD ECON. F. (Apr. 17, 2019), https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f [https://perma.cc/ZT8G-4VPF].

[58] ZUBOFF, *supra* note 51, at 80–81.

[59] See, e.g., Bass v. Facebook, Inc., 394 F. Supp. 3d 1024, 1028 (N.D. Cal. 2019) (noting that 96% of Facebook's revenue comes from targeted advertising). In 2018 alone,

resulting market is staggering in scale: In 2019, a handful of dominant social media platforms in the United States had a market capitalization of more than four trillion dollars.[60] They, like other firms that capture data, feed into a multi-million dollar secondary market of "brokers" that buy and sell that personal data.[61] The resulting economic logic of data "extraction, processing, and execution that characterizes surveillance capitalism" creates a direct causal link between the ability to capture personal data and the potential for economic profit through behavioral advertising.[62] Given the scale of potential profit, platforms and many other firms have powerful incentives to maximize the collection of personal data.[63] Moreover, identifying pregnant people, even those who do not want to be identified, is a particularly lucrative advertising opportunity because becoming a new parent is one of the few life changes that leads to new purchasing habits.[64]

To be sure, this does not mean that firms never willingly forego such collection. Apple's decision to install end-to-end encryption on its message app is an instance of consumer demand for privacy outstripping the firm's pecuniary interest in data.[65] Apple and Google have also made storage encryption a default on their more recent operating systems.[66] Apple, however, also "publicly touts how its busi-

---

Facebook made $55.8 billion in revenue, mostly from its advertising business. *Facebook Reports Fourth Quarter and Full Year 2018 Results*, FACEBOOK (Jan. 30, 2019), https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx [https://perma.cc/X3X9-8ENN]. *See generally* Sarah Myers West, *Data Capitalism: Redefining the Logics of Surveillance and Privacy*, 58 BUS. & SOC'Y 20 (2019) (describing the historical development of targeted advertising markets).

[60] LUIGI ZINGALES & FILIPPO MARIA LANCIERI, U. CHI. BOOTH SCH. BUS. STIGLER CENTER, STIGLER COMMITTEE ON DIGITAL PLATFORMS, FINAL REPORT 6 (2019).

[61] Matthew Crain, *The Limits of Transparency: Data Brokers and Commodification*, 20 NEW MEDIA & SOC'Y 88, 98 (2016); *see also* Huq, *supra* note 51, at 346–47 (discussing the distinctive role of data brokers in the digital economy).

[62] Mariano-Florentino Cuéllar & Aziz Z. Huq, *Economies of Surveillance*, 133 HARV. L. REV. 1280, 1288 (2020) (book review).

[63] *See* ZUBOFF, *supra* note 51, at 74–92 (recounting how Google gave up on a model of limited data collection under pressure from its private investors).

[64] *See, e.g.*, Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/4ZVN-BUAU] ("And among life events, none are more important than the arrival of a baby. At that moment, new parents' habits are more flexible than at almost any other time in their adult lives.").

[65] *See* Caitlin Dewey, *Apple's iMessage Encryption Foils Law Enforcement, Justice Department Complains*, WASH. POST (Apr. 5, 2013), https://www.washingtonpost.com/business/technology/apples-imessage-encryption-foils-law-enforcement-justice-department-complains/2013/04/05/f4a6b66e-9d68-11e2-a2db-efc5298a95e1_story.html [https://perma.cc/NKW9-EHHC].

[66] *See* Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 576 (2018).

ness model doesn't need to access user data" in ways that underscore how its commercial incentives diverge sharply from those of its competitors.[67]

Notwithstanding such examples, it seems reasonable to anticipate that, even in a post-*Dobbs* world, many commercial actors will heed the powerful financial incentives created by surveillance capitalism to capture personal data about pregnant people either for their own internal uses or for sale on the secondary market. We return in Part III to the question of whether there are countervailing pressures that might curb these appetites at least for some firms.

B. The Patient's Search

Access to reproductive care interacts with these data-based economies in three main ways: (1) through the collection and use of biometric data, including by self-tracking tools; (2) through the role that search engines and social networks play in information acquisition; and (3) through the increasing pervasiveness of location-tracking tools.

To begin with, patients increasingly obtain information about the fact and the development of a pregnancy through mobile devices that engage in "self-tracking." This involves the collection and analysis of biometric data about patients' "wellness and health" through wearable devices.[68] About one in five Americans uses a smart watch or wearable fitness tracker.[69] By gathering data on exercise, diet, and more, self-tracking apps enable individuals (or third parties such as spouses, employers, or physicians) to take preemptive action in respect to their health.[70]

Most relevant here are period tracking apps, which gather information on menstrual cycles, moods, fetal movements, and more.[71]

---

[67] Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 116–17 (2018).

[68] GINA NEFF & DAWN NAFUS, SELF-TRACKING 2 (2016).

[69] Emily A. Vogels, *About One-in-Five Americans Use a Smart Watch or Fitness Tracker*, PEW RSCH. CTR. (Jan. 9, 2020), https://www.pewresearch.org/fact-tank/2020/01/09/about-one-in-five-americans-use-a-smart-watch-or-fitness-tracker [https://perma.cc/5PUB-3U4L].

[70] *See* Stine Lomborg & Kirsten Frandsen, *Self-tracking as Communication*, 19 INFO. COMMC'N & SOC'Y 1015, 1017 (2016) ("A key idea is that self-tracking, because of its making visible patterns regarding calorie intake, exercise, sleep and so on, may be seen as a resource for empowering the individual user vis-à-vis health-care professionals.").

[71] Vanessa Rizk & Dalia Othman, *Quantifying Fertility and Reproduction Through Mobile Apps: A Critical Overview*, 22 ARROW FOR CHANGE 13, 13–14 (2016); *see also* Donna Rosato, *What Your Period Tracker App Knows About You*, CONSUMER REPS. (Jan. 28, 2020), https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you [https://perma.cc/PE8T-7NYE] (explaining that period trackers are

Some can predict a pregnancy "on average nine days before at-home pregnancy tests."[72] Almost one-third of women in the United States have used or now use period-tracking apps.[73] Other apps also track menstrual cycles, but "for the benefit of [a] partner[]."[74] Another part of the multi-billion dollar workplace wellness industry[75] allows employers to purchase self-tracking tools for their workers, retaining access to, and even sharing with insurers, the data thereby generated.[76] For example, Progyny is a very profitable company that manages fertility benefits for employees at large companies.[77] Other apps marketed directly to employers "focus on the aspects of women's health linked to reproduction, including menstruation, fertility, pregnancy, and menopause."[78]

Second, after a person starts to suspect or confirms the fact of a pregnancy, they may seek out information about their medical options. Patients' search for information about reproductive care and access to services likely transpires through online search engines such as Google.[79] When patients transact with providers or secure prescriptions online, this also generates data trails: search histories associated with a person's internet protocol (IP) address; details of any financial

helpful tools for monitoring menstrual cycle problems, preventing pregnancy, and getting pregnant).

[72] *Wearable Devices Measure a Growing Array of Health Indicators*, ECONOMIST (May 2, 2022), https://www.economist.com/technology-quarterly/2022/05/02/wearable-devices-measure-a-growing-array-of-health-indicators [https://perma.cc/7FF5-DCDX].

[73] Rosato, *supra* note 71.

[74] Karen E.C. Levy, *Intimate Surveillance*, 51 IDAHO L. REV. 679, 685 (2015).

[75] *See Corporate Wellness Market Size, Share & Trends Analysis Report by Service (Health Risk Assessment, Fitness), by End Use, by Category, by Delivery Model (Onsite, Offsite), by Region, and Segment Forecasts, 2022-2030*, GRAND VIEW RSCH., https://www.grandviewresearch.com/industry-analysis/corporate-wellness-market [https://perma.cc/7AUY-G4CS] (reporting that the industry was worth $51 billion in 2021).

[76] *See* Patience Haggin, *As Wearables in Workplace Spread, So Do Legal Concerns*, WALL ST. J. (Mar. 13, 2016), https://www.wsj.com/articles/as-wearables-in-workplace-spread-so-do-legal-concerns-1457921550 [https://perma.cc/S7VZ-Y8AR] (noting that wearable devices allow employers to track workers' productivity and collect data about their health). Firms can obtain discounts on insurance costs by agreeing to share employees' data with an insurer. *See* Jonah Comstock, *Employer Gets $280k Insurance Discount for Using Fitbits*, MOBI HEALTH NEWS (July 15, 2014, 9:20 AM), https://www.mobihealthnews.com/34847/employer-gets-280k-insurance-discount-for-using-fitbits [https://perma.cc/8BHV-R7JT].

[77] Heather Landi, *Progyny Brings in $9.6M in Profits but Misses Wall Street Estimates*, FIERCE HEALTHCARE (Mar. 6, 2020, 8:23 AM), https://bit.ly/2TGeqqY [https://perma.cc/6WNB-2NG6].

[78] Elizabeth A. Brown, *The Femtech Paradox: How Workplace Monitoring Threatens Women's Equity*, 61 JURIMETRICS J. 289, 306 (2021).

[79] *See* Conti-Cook, *supra* note 37, at 22–28 (noting that pregnant people often turn to searching online to get information on their reproductive health).

dealings; and details of any medication and procedures researched or obtained.

The quality of the search results hinges on several structural decisions firms need to make about the architecture of their applications. To begin with, search algorithms can do a better or worse job of screening for false or misleading information. One study by the Center for Countering Digital Hate found that 37% of Google Maps results and 11% of Google searches for "abortion clinic near me" and "abortion pill" in presently restrictive states directed users to "crisis pregnancy centers" or "pregnancy resource centers." These do not provide abortions and instead "oppose abortions, shame abortion care, or promote alternatives to abortion."[80] Pro-life pregnancy centers have a record of "threshold deception that attracts women to pregnancy centers" and "misinformation . . . once they walked through a pregnancy center's doors."[81]

Even though these search results arise from the automated operation of Google's PageRank algorithm, they are self-evidently in some tension with the premise that the algorithm matches users to what *they* want to see, as opposed to what a third party wants them to see. It seems implausible that patients are seeking misleading information on reproductive health when they go online.[82]

Further, social media networks' content moderation decisions will also shape the epistemic environment. After *Dobbs*, for example, Facebook and Instagram both promptly removed posts offering abortion medication.[83] Even truthful statements such as "abortion pills can be mailed" have been removed by content-moderation algorithms.[84]

---

[80] *Google Directs Users to Anti-Abortion 'Fake Clinics*,' CTR. FOR COUNTERING DIGIT. HATE (June 9, 2022), https://counterhate.com/research/anti-abortion-fake-clinics [https://perma.cc/2BYW-PBNQ].

[81] Hayley E. Malcolm, Note, *Pregnancy Centers and the Limits of Mandated Disclosure*, 119 COLUM. L. REV. 1133, 1136 (2019).

[82] That said, we recognize that confirmation bias can skew search efforts even in respect to health data. For evidence on this point in the context of childhood vaccines, see Corine S. Meppelink, Edith G. Smit, Marieke L. Fransen & Nicola Diviani, *"I Was Right About Vaccination": Confirmation Bias and Health Literacy in Online Health Information Seeking*, 24 J. HEALTH COMMC'N 129, 129–30 (2019). Our point here is that there is likely to be a substantial number of people searching for reproductive health information who do not want distorted information.

[83] *Instagram and Facebook Begin Removing Posts Offering Abortion Pills*, NPR (June 28, 2022, 12:27 AM), https://www.npr.org/2022/06/28/1108107718/instagram-and-facebook-begin-removing-posts-offering-abortion-pills [https://perma.cc/G6TG-E4N9] ("Facebook and Instagram have begun promptly removing posts that offer abortion pills to women who may not be able to access them following a Supreme Court decision that stripped away constitutional protections for the procedure.").

[84] Katharine Trendacosta, *Abortion Information Is Coming Down Across Social Media. What Is Happening and What Next.*, ELEC. FRONTIER FOUND. (July 28, 2022), https://

The alacrity of platforms' censorship efforts respecting abortion contrasts with comparatively ineffectual takedown policies respecting racial hate speech.[85] The increasing use of algorithmic tools to manage content moderation also means that the relative priority of different speech prohibitions on a platform is unlikely to be apparent to casual users.[86] Nor will it be clear whether these differences flow from deliberate policy choices or are inadvertent effects of content-moderation systems. Indeed, they may not be legible without sophisticated empirical inquiries. Beyond these concerns, online access to information and services depends on internet service providers (ISPs) facilitating such access. But ISPs have in the past "throttled" access to certain sites.[87] Alternatively, a content delivery network (CDN) might decide to withdraw protection from cyberattacks, which often aim at disabling the site and hence preventing access by internet users.[88] Further, service providers can limit access to sites at the domain-name system level such that sites are never accessible from other parts of the internet.[89] The federal government has also seized domain names, "changing the pointer in the routing system to the Justice Department web site."[90]

---

www.eff.org/deeplinks/2022/07/abortion-information-coming-down-across-social-media-what-happening-and-what-next [https://perma.cc/JS65-W84Z].

[85] About half of the misogynistic and racist posts that violate Facebook's community standards are not taken down, even when they are reported to the company. *See* Caitlin Ring Carlson & Hayley Rousselle, *Report and Repeat: Investigating Facebook's Hate Speech Removal Process*, First Monday (Feb. 2020), https://journals.uic.edu/ojs/index.php/fm/article/view/10288/8327 [https://perma.cc/6LFA-HHDZ].

[86] *See* Robert Gorwa, Reuben Binns & Christian Katzenbach, *Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance*, Big Data & Soc'y, Jan.–June 2020, at 2, 10–11 (noting concerns about the transparency of moderation algorithms).

[87] Andrea M. Matwyshyn, *Unavailable*, 81 U. Pitt. L. Rev. 349, 369 (2019) (noting that certain access plans are "contractually subject to throttling in the sole discretion of [ISPs such as] Verizon").

[88] For a discussion of some attack tools, see *What is a DDoS Attack?*, Cloudflare, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack [https://perma.cc/L697-ZY7K] (explaining how DDoS attacks function and how to mitigate them).

[89] *See How Does DNS Filtering Work?*, WebTitan (Jan. 30, 2021), https://www.spamtitan.com/web-filtering/how-does-dns-filtering-work [https://perma.cc/YQT2-RDB2].

[90] Mark A. Lemley, *The Splinternet*, 70 Duke L.J. 1397, 1416 (2021). Had it been enacted, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property (PROTECT IP) Act of 2011, S. 968, 112th Cong. (2011), would have permitted a court to issue temporary restraining orders or injunctions against domain names and mandated domain-name system filtering. *See* Steve Crocker, David Dragon, Dan Kaminsky, Danny McPherson & Paul Vixie, *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill* (May 2011), https://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf [https://perma.cc/RT6B-QYFC] (describing the security concerns associated with domain-name system filtering).

The transaction costs and results of patient search, in short, hinge to a large extent on firms' decisions about the architecture of online access to information. Their architectural choices, however, will largely be opaque to patients.

Third, state-level prohibitions on abortion create an incentive for those seeking reproductive care to cross state borders and seek services in another jurisdiction. The search for services need not explicitly rely on digital tools, like the search for information via search engines, to leave a digital trace. As we have noted, individuals' movements generate digital traces because of the presence of location-tracking capabilities in phones, wearable devices, and vehicles. Unless a patient makes a conscious decision to avoid generating such digital data trails, it is very likely that they will inadvertently create a record of their activities.[91] For example, the use of an Alphabet app generates locational data because the company logs GPS data "about every two minutes" so long as one of its apps is in use on a phone.[92] A person who uses Google Maps, or communicates via Google Chat, while physically accessing an abortion-related service generates a corresponding data trail even if they are not using those apps for the purpose of securing such access. And a person who does not realize that their apps are generating and sharing these data will unwittingly create a record of their search for abortion-related information and services.

C. The Restrictionist's Search

"Law enforcement, civil or criminal, depends on information."[93] Because so much patient activity occurs online, or alternatively generates a digital data trail, the antiabortion prosecutor (or, indeed, civil plaintiff under certain circumstances) is likely to begin their search not solely with eyewitness interviews or physical evidence but also by looking for the electronic traces of patient search.[94] Prosecutors and

---

[91] In practice, it is extremely difficult to preserve anonymity given the penetration of the digital economy into daily life. *See If You Think You're Anonymous Online, Think Again*, NPR (Feb. 24, 2014, 11:00 AM), https://www.npr.org/transcripts/282061990 [https://perma.cc/95J6-KK6Q] (discussing efforts by journalist Julia Angwin to remove her presence online).

[92] Bobby Allyn, *Privacy Advocates Fear Google Will Be Used to Prosecute Abortion Seekers*, NPR (July 11, 2022, 5:00 AM), https://www.npr.org/2022/07/11/1110391316/google-data-abortion-prosecutions [https://perma.cc/NN9L-CY2A].

[93] William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1029 (1995); *accord* Miriam H. Baer, *Law Enforcement's* Lochner, 105 MINN. L. REV. 1667, 1670 (2021) ("[E]nforcement relies heavily on information.").

[94] *Cf.* Daniel C. Richman, *Framing the Prosecution*, 87 S. CAL. L. REV. 673, 676 (2014) (noting ongoing reliance on eyewitnesses despite developments of the surveillance state).

civil plaintiffs wanting to identify patients who have sought or intend to seek reproductive care covered by a restrictionist state statute can exploit this rich digital environment by following the data trail left by a pregnant person. This allows them to "mirror," and hence recreate, an inventory of the pregnant person's activities, movements, conversations, and perhaps even thoughts.

This process is appropriately called "mirroring" because it involves retracing the pregnant person's steps and gathering data that acts as a "mirror" of that person's earlier activities. The advent of machine-learning instruments for inferring new facts from large volumes of data, in addition, allows inferences about pregnancy even when the person concerned has not tracked their own biometric data, used online search tools, or created locational traces. The use of predictive inference to identify abortion access supplements the use of personal data as a revelatory mirror of earlier online and physical activity.

1. Following the Data Trails Using Compulsory Legal Process

Consider first the ways in which law enforcement can access the biometric and internet-use-related data generated by patients. In respect to these forms of data, prosecutors can avail themselves of "[s]earches of digital devices" as an "increasingly common form of surveillance."[95] If prosecutors do not have the device in question, they can instead directly secure data from tech firms such as ISPs and search providers. Google alone receives tens of thousands of requests annually from law enforcement.[96] Law enforcement can obtain warrants, which are issued on the basis of a showing of probable cause. They can obtain wiretap orders to require real-time disclosures of such data as it is being created.[97] And, although controversial and subject to ongoing Fourth Amendment challenges, they can use geofence warrants to compel disclosures of information about everyone who passed through a particular location at a particular time, or searched the web for a particular keyword.[98] A geofence warrant "[S]pecifies a location and period of time, and, after judicial approval, companies

[95] Conti-Cook, *supra* note 37, at 29.

[96] *See* Google Transparency Report, *Global Requests for User Information*, GOOGLE, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:US [https://perma.cc/8GNY-V3MS]; *see also infra* text accompanying notes 123–46 (offering more precise data by type of search request).

[97] *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2516 (authorizing the interception of wire, oral, or electronic communications with a court order).

[98] *Cf.* United States v. Chatrie, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022) (invalidating warrant on Fourth Amendment grounds).

conduct sweeping searches of their location databases and provide a list of cell phones and affiliated users found at or near a specific area during a given timeframe . . . ."[99]

Moreover, warrants are not the only or the easiest search tool. A grand jury subpoena allows a federal investigator to obtain "documentary or digital evidence with almost no constitutional limitation other than a watered down version of the Fourth Amendment reasonableness requirement."[100] Similarly, an administrative subpoena can be secured without a showing of probable cause.[101] These cannot be used for all forms of data. Data classified as content generally requires a warrant for government access.[102]

Yet even when it comes to content data, warrants will offer only very limited protection against restrictionist law enforcement demands. Where a warrant is required, the Fourth Amendment hitches the scope of police search authority to the scope of substantive criminal law. A probable cause determination requires a magistrate to consider whether there is evidence pertaining to the elements of a cited criminal law.[103] Of course, restrictionist prosecutors will be able to point to criminal statutes in seeking evidence about abortion. And the broader those laws, the easier it will be to show probable cause. As a result, there will be many instances in which a warrant will not be difficult to obtain because there is a readily pertinent and applicable statutory hook for probable cause.[104] Indeed, the linkage between the scope of criminal law and the reach of lawful search authority creates

---

99 Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2509 (2021) [hereinafter *Geofence Warrants*]; *see also In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 734–75 (N.D. Ill. 2020) (holding that a warrant is required for geofence data).

100 Baer, *supra* note 93, at 1699 (discussing United States v. R. Enters., Inc., 498 U.S. 292, 299 (1991)).

101 *See* United States v. Morton Salt Co., 338 U.S. 632, 652 (1950) ("[I]t is sufficient if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant."); *see also* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 218 (1946) ("No sufficient reason was set forth . . . for not enforcing the subpoenas . . . .").

102 *See* United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) (finding that a criminal defendant had a reasonable expectation of privacy in the content of his emails for Fourth Amendment purposes). On the influence of the *Warshak* court's reasoning beyond the Sixth Circuit, see Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 400 (2014).

103 *Cf.* Aziz Z. Huq, *How the Fourth Amendment and the Separation of Powers Rise (and Fall) Together*, 83 U. CHI. L. REV. 139, 149 (2016) ("The reference to probable cause . . . is an incorporation by reference of substantive criminal law.").

104 For further consideration on the abiding ambiguity about what "probable cause" entails, compare Andrew Manuel Crespo, *Probable Cause Pluralism*, 129 YALE L.J. 1276, 1280 (2020) ("Existing probable-cause jurisprudence says almost nothing at all about either the methodology or the substance of the judge's inquiry: *how* should the judge go about

an incentive for legislatures to expand the scope of criminal liability in relation to reproductive care. Inchoate and complicity-based forms of criminal liability, for example, may come to be viewed as desirable simply because of how they facilitate lawful search.

Under federal statutory law, heightened protections apply to certain elements of the data trails left by pregnant persons. But these statutes tend to have law-enforcement exceptions that authorize disclosure pursuant to legal process.[105] Under a Privacy Rule issued pursuant to the Health Information Portability and Accountability Act (HIPAA),[106] disclosures by covered providers are prohibited absent a court order, subpoena, or warrant. Further, there is an additional exception for law enforcement, which allows disclosures that are otherwise required by legal process.[107] On June 29, 2022, the Department of Health and Human Services issued guidance clarifying, but not changing, the scope and limits of disclosure under the HIPAA Privacy Rule.[108] Health data can also be reidentified without violating the HIPAA Privacy Rule.[109] Nevertheless, what limited protections HIPAA affords only cover traditional healthcare providers, health plans, and health care clearinghouses—and not most digital apps.[110]

Similarly, the Gramm-Leach-Bliley Act prohibits disclosures of personal financial information, but carves out the release of informa-

---

determining the strength of the government's assertions? And *what* counts as strong enough?").

105 *See generally* Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 UCLA L. Rev. 212 (2021) (discussing the imbalance between exceptions in privacy statutes for law enforcement but not for criminal defense investigators); Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exceptions*, 111 Mich. L. Rev. 485 (2013) (discussing the political economy of law enforcement exceptions in privacy statutes).

106 *See* 45 C.F.R. §§ 160, 164.102–.106, 164.400–.414 (2021).

107 *See id.* § 164.512(f)(1)(2021) (permitting covered entities to disclose PHI about an individual for law enforcement purposes "[p]ursuant to process and as otherwise required by law" under certain conditions).

108 *See HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, U.S. Dep't of Health & Hum. Servs. (June 29, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html [https://perma.cc/628S-F3XB] (clarifying that regulated entities can disclose personal reproductive health information "*only* as expressly permitted or required by the Privacy Rule").

109 *See* I. Glenn Cohen & Michelle M. Mello, *Big Data, Big Tech, and Protecting Patient Privacy*, 322 JAMA 1141, 1141 (2019) (explaining how reidentification could be done "if Google identified individuals by linking EHR data without HIPAA identifiers to internet data of consumers who visited the University of Chicago hospital and searched online for information about particular medical conditions").

110 *See Covered Entities and Business Associates*, U.S. Dep't of Health & Hum. Servs. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/MQB6-TFQH] ("If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA Rules.").

tion upon legal process by law enforcement.[111] Under the federal Stored Communications Act (SCA) regime,[112] which applies to electronic communication service providers, there are a set of complex distinctions between content and noncontent elements of covered communications.[113] The SCA restricts electronic communications service providers' voluntary disclosure of the contents of stored communications, such as emails or chat messages.[114] But it too contains similar law enforcement exceptions,[115] and no restrictions whatsoever on the ability of private entities to compel the disclosures of noncontent data.[116] In short, entities covered by HIPAA, Gramm-Leach-Bliley, and the SCA may be barred from some voluntary disclosures but they must still respond to criminal investigations and, in many instances, to civil subpoenas.[117]

We note that private firms are not the only entities in possession of relevant information. States also maintain large stocks of locational data because they manage highway toll systems and surveillance cameras. Under current law, that data can also be secured through legal process, and used in coercive actions. In Illinois, for example, E-Z Pass data has been disclosed through civil process in divorce proceedings.[118] The regulation of such state-held data, of course, will be a matter of state law. Whether and how a pro-choice state such as Illinois will disclose its data to neighboring states engaged in antiabortion prosecutions remains to be seen.

---

111 15 U.S.C. § 6802(e)(5) (creating an exception for "law enforcement agencies[,] including the Bureau of Consumer Financial Protection"). Note that the statute is ambiguous as to whether this refers to solely federal entities, or both federal and state law-enforcement.

112 18 U.S.C. §§ 2701–2711 (regulating access to stored communications).

113 For an overview of the statute, see Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004). Parts of the SCA were struck down in *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), and the interaction between that decision and the remaining statutory text presents complex questions.

114 18 U.S.C. § 2702.

115 *See id.* §§ 2702–2703 (permitting a government entity to require disclosure of communications with a warrant, subpoena, or court order).

116 *See id.* (regulating only government entities).

117 State privacy law in the five states with comprehensive schemes tends to follow the same pattern. *See* Jake Holland, *Abortion Access Data and State Consumer Privacy Laws: Explained*, BLOOMBERG L. (July 11, 2022, 5:30 AM), https://news.bloomberglaw.com/privacy-and-data-security/abortion-access-data-and-state-consumer-privacy-laws-explained [https://perma.cc/MMY2-CGF4].

118 Tony Arnold, *How Your Private Illinois Tollway Data Is Shared With Cops and Divorce Lawyers*, WBEZ (Sept. 19, 2019, 10:19 AM), https://www.wbez.org/stories/how-your-private-illinois-tollway-data-is-shared-with-cops-and-divorce-lawyers/cea68ea0-4b13-481a-80a1-50bf0e9db738 [https://perma.cc/65L8-LMUJ].

Where the prosecutor cannot or does not wish to seek a warrant to obtain information from an ISP or the like, a grand jury subpoena, administrative subpoena, or a number of other options are open. The technically sophisticated may be tempted "to employ creative and novel methods to circumvent or 'workaround' these protections, like exploiting encryption vulnerabilities or backdoors" in order to access data.[119] One such tactic may be to use "malware," or "software designed to conduct surreptitious surveillance on a target's computer or network" to access information.[120] Of course, another possibility is for the state to simply purchase the data outright—a possibility we consider at greater length in the next Section.[121]

The final kind of data trail—locational information—is subject to a slightly different legal regime that we should mention. In 2018, the Supreme Court ruled that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site locational data]."[122] To the extent that this holding is applied to other forms of locational data, it means that a warrant regime will apply there. Again, this requirement is likely to be easily satisfied.

2. Data Supply Absent Compulsory Legal Process

In coming conflicts over reproductive choice, two kinds of regulators will seek to surveil pregnant people and abortion providers and to acquire data about individuals' private medical choices. One will be police and prosecutors (collectively, "law enforcement") in antiabortion states. The other will be nongovernmental "vigilantes"[123] aiming either to collect data and hand it over to law enforcement, or to bring civil lawsuits directly against any person who facilitates an abortion pursuant to the aiding and abetting provisions of some states'

---

[119] Jonathon W. Penney & Bruce Schneier, *Platforms, Encryption, and the CFFA: The Case of* WhatsApp v. NSO Group, 36 BERKELEY TECH. L.J. 469, 472 (2021); *see also* Mayer, *supra* note 66, at 586–88 (discussing how law enforcement investigators take advantage of applications' and mobile devices' vulnerabilities to external hacks). While law enforcement's use of hacking tools is strictly regulated, private vigilantes could engage in these investigative tactics and then launder the results through data brokers or volunteer them directly to police. *See infra* text accompanying notes 143–42 (discussing the Anonymous hacking collective).

[120] Paul Ohm, *The Investigative Dynamics of the Use of Malware by Law Enforcement*, 26 WM. & MARY BILL RTS. J. 303, 312 (2017).

[121] This assumes it is not already in the public domain, or in another agency's archives. *See* Murphy, *supra* note 105, at 519–21 (discussing federal statutory frameworks covering information sharing by law enforcement).

[122] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[123] For a penetrating analysis of this phenomenon, see Jon D. Michaels & David L. Noll, *Vigilante Federalism*, 108 CORNELL L. REV. (forthcoming 2023).

antiabortion statutes.[124] There are a variety of routes for these groups to acquire abortion-relevant data without resort to compulsory legal process. In this Section, we summarize four different pathways: the private market for data; voluntary non-commercial disclosures by private actors; hacking; and inferences derived from the use of machine-learning tools.

To start with, anyone from either group can purchase data from data brokers on the open market.[125] Both private data brokers and "private companies such as pizza chains and contact lens companies" offer police data for sale.[126] As recently as May 2022, *Vice News* reportedly bought a week's worth of location data for people visiting Planned Parenthood for slightly over $160 from a data broker called SafeGraph.[127] Data brokers like SafeGraph obtain and aggregate location data from a variety of sources, including cell phone apps that have location services enabled.[128] While the data are often nominally anonymized, deanonymization is technically feasible.[129] Even in the wake of *Dobbs*, more than two dozen data brokers continued to market information about expecting parents in the United States.[130] They ignored calls from Democratic lawmakers to limit the circulation of such data given concerns that it would imperil reproductive choice.[131] Recent research by the Center for Democracy and Technology finds that law enforcement and intelligence agencies spend millions on purchases of private-sector data from data bro-

---

124 *See, e.g.*, Texas Heartbeat Act, S.B.8, 87th Leg., Reg. Sess. (Tex. 2021) (codified at TEX. HEALTH & SAFETY CODE ANN. § 171.208(a)(1)–(2) (West 2021)); *see infra* text accompanying notes 203–04 (discussing that statute).

125 *See, e.g.*, Bennett Cyphers, *How the Federal Government Buys Our Cell Phone Location Data*, ELEC. FRONTIER FOUND. (June 13, 2022), https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data [https://perma.cc/4CAM-F5WR].

126 Sarah Brayne, *The Criminal Law and Law Enforcement Implications of Big Data*, 14 ANN. REV. L. & SOC. SCI. 293, 301 (2018).

127 Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE: MOTHERBOARD (May 4, 2022, 1:46 AM), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood [https://perma.cc/CE6L-FLJA].

128 *See generally* SARAH LAMDAN, DATA CARTELS: THE COMPANIES THAT CONTROL AND MONOPOLIZE OUR INFORMATION 30 (2022) (describing the emergence of "data analytics" or "business solutions" firms that control the flow of information generated through digital activity).

129 Cox, *supra* note 127.

130 Alfred Ng, *Data Brokers Resist Pressure to Stop Collecting Info on Pregnant People*, POLITICO (Aug. 1, 2022, 4:20 PM), https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988 [https://perma.cc/U7XA-CBWE].

131 *Id.*

kers.[132] This evidence, while anecdotal, suggests that data brokers have systematically different incentives from other firms in the digital economy. They do not gather data directly from consumers and have no incentive to retain consumers' trust. Instead, their profit is linked to the low cost of data acquisition and the high price commanded by the aggregated data that they then sell on.

A bill pending in Congress as of this publication, called the Fourth Amendment Is Not For Sale Act, would bar governmental entities from circumventing warrant requirements by purchasing Fourth Amendment-protected information via commercial markets.[133] The SCA's existing bar on technology companies providing voluntary disclosures of communications content data to law enforcement absent service of legal process offers a precedent for such a move.[134] But this bill would probably clash with law enforcement's longstanding practice of purchasing information from confidential informants and offering monetary rewards for investigative leads.[135] As a result of such tensions with longstanding (and generally accepted) practices, it is unclear whether the bill is ultimately likely to be enacted into law in current form.[136] Even if the bill did become a federal statute, it would have no effect on nongovernmental purchasers—such as the vigilante plaintiffs seeking to use damages actions against patients and providers, or seeking to facilitate a prosecutor's actions by sharing resources with them.

Second, some big tech firms may go further and affirmatively volunteer data to restrictionist law enforcement or vigilante groups free of charge. Technology companies have done this before at scale. Multiple major technology companies have either voluntarily or in response to political pressure implemented automated systems to scan

---

[132] Sharon Bradford Franklin, Greg Nojeim, Dhanaraj Thakur & Carey Shenkman, Ctr. for Democracy & Tech., Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers 7 (Dec. 2021), https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers [https://perma.cc/JB77-B7P9].

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

[134] *See* Orin S. Kerr, Hoover Working Grp. on Nat'l Sec., Tech., & L., Aegis Series Paper No. 2109, Buying Data and the Fourth Amendment 9 (2021), https://www.lawfareblog.com/buying-data-and-fourth-amendment [https://perma.cc/W8TT-YBAV].

[135] On the role of informants in the criminal justice system, see Ariel C. Werner, *What's in a Name? Challenging the Citizen-Informant Doctrine*, 89 N.Y.U. L. Rev. 2336 (2014). On the historical pedigree of rewards, see L. Radzinowicz, *Trading in Police Services: An Aspect of the Early 19th Century Police in England*, 102 U. Pa. L. Rev. 1, 5 (1953).

[136] We note that it is possible to distinguish in statutory text between entities that engage in the sale of data as the primary business, and persons who engage in occasional transactions.

emails, chat messages, attachments, and cloud storage account contents for "hashes," or digital fingerprints, associated with known child sexual abuse materials (CSAM).[137]

Under Apple's policy, for example, if the automated system identifies a positive match, company personnel will review the allegedly infringing file and, if it is confirmed as contraband, alert the police.[138] For another example, police in California famously identified a serial murderer, the Golden State Killer, by using an online service called GEDmatch to compare DNA from a crime scene against DNA profiles that users had voluntarily uploaded.[139] Anyone can access GEDmatch for free.[140] Yet a third example is a nonprofit organization that builds internet surveillance software, and then donates licenses to law-enforcement organizations around the world, that can identify CSAM on the dark web.[141] Technology companies with antiabortion sympathies could easily volunteer similar free services to track abortion-relevant data across the internet and hand it over to law enforcement or vigilante civil society groups. If a firm or a data broker—perhaps acting out of restrictionist sentiments—decides to offer up information for free, they are permitted to do so unless covered by the HIPAA Privacy Rule, Gramm-Leach-Bliley, SCA, or an analogous state rule.[142]

Next, private actors could also engage in hacking campaigns to bypass digital security and access sensitive data illegally.[143] This, too,

---

[137] *See Expanded Protections for Children: Frequently Asked Questions*, APPLE (Aug. 2021), https://www.apple.com/child-safety/pdf/Expanded_Protections_for_Children_Frequently_Asked_Questions.pdf [https://perma.cc/B2XQ-VTDN] (outlining Apple's company policy for detecting CSAM); *cf.* Michael H. Keller & Gabriel J.X. Dance, *Child Abusers Run Rampant as Tech Companies Look the Other Way*, N.Y. TIMES (Nov. 9, 2019) https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html [https://perma.cc/RJS4-ZW8P].

[138] *Id.*

[139] Gina Kolata & Heather Murphy, *The Golden State Killer Is Tracked Through a Thicket of DNA, and Experts Shudder*, N.Y. TIMES (Apr. 27, 2018), https://www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html [https://perma.cc/7UAG-PK8R].

[140] GEDMATCH, https://www.gedmatch.com [https://perma.cc/5XA5-FVJL].

[141] *About Us*, CHILD RESCUE COAL., https://childrescuecoalition.org/about-us [https://perma.cc/8J7C-5KRP].

[142] A July 8, 2022 executive order encourages the Federal Trade Commission to consider actions "appropriate and consistent with applicable law . . . to protect consumers' privacy when seeking information about and provision of reproductive healthcare services." Exec. Order No. 14,076, 87 Fed. Reg. 42053 (July 8, 2022). It remains to be seen whether this hortatory language yields any material change to firms' options.

[143] *Cf.* Kashmir Hill, *Data Broker Was Selling Lists of Rape Victims, Alcoholics, and 'Erectile Dysfunction Sufferers'*, FORBES (Dec. 19, 2013, 3:40 PM), https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/#42acebdb1d5 [https://perma.cc/H6LL-L5JN].

has concrete precedents. For instance, members of the Anonymous hacker collective notoriously hacked a website to collect and leak evidence of a rape and coverup allegedly perpetrated by members of the Steubenville, Ohio, high school football team.[144] It is not hard to imagine similar conduct by antiabortion hacking groups targeting, say, a Planned Parenthood clinic. These entities could either use the data acquired themselves in civil prosecutions under S.B.8 or the like, or else obscure unlawful origins by redistributing it to law enforcement or other nongovernmental regulators without disclosing the source.

Or consider the phenomenon of "stalkerware": Abusive intimate partners and exes have downloaded apps to millions of unaware victims' phones that enable stalkers to remotely access a phone's "photos, videos, texts, calls, voice mails, searches, social media activities, locations . . . [and to] activate a phone's mic to listen to conversations within 15 feet of the phone."[145] Post-*Dobbs*, stalkerware can enable stalkers to collect incriminating evidence of their victims' intimate healthcare choices, "enabling their imprisonment."[146] The restrictionist legal regime, in this way, once again enables and elicits the use of private violence against the pregnant.

3. Inferring Pregnancy and Abortion Information

But what if facts about an individual's pregnancy could be inferred from data that had no prima facie connection to that condition? Over a decade ago, the retailer Target made the news for its "pregnancy-prediction model," which applied data analytics to shoppers' consumption behavior to predict the fact of a pregnancy.[147] In the subsequent decade, the computational technique of "machine learning," which is used to mine large pools of data for unanticipated

---

144 The hackers ultimately faced more prison time than the individuals convicted of rape. Mohit Kumar, *Hacker Who Exposed Steubenville Rape Faces Longer Prison Term Than Rapists*, HACKER NEWS (Nov. 28, 2016), https://thehackernews.com/2016/11/steubenville-rape-hacker.html [https://perma.cc/KV4Q-QQW3].

145 Danielle Keats Citron, *Abortion Bans Are Going to Make Stalkerware Even More Dangerous*, SLATE (July 5, 2022, 8:00 AM), https://slate.com/technology/2022/07/stalkerware-abortion-bans-privacy.html [https://perma.cc/MF9Y-947Z] [hereinafter Citron, *Abortion Bans*]; *see also* Lorenzo Franceschi-Bicchierai & Joseph Cox, *Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones*, VICE: MOTHERBOARD (Apr. 18, 2017, 1:01 PM), https://www.vice.com/en/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x [https://perma.cc/Y7L7-LMAC] (reporting on the popularity of consumer spyware usage by intimate partners). For an insightful academic discussion on consumer surveillance apps, see Danielle Keats Citron, *Spying Inc.*, 72 WASH. & LEE L. REV. 1243, 1244–47 (2015).

146 Citron, *Abortion Bans*, *supra* note 145.

147 Duhigg, *supra* note 64.

correlations and inferences, has improved dramatically.[148] Using machine learning tools, otherwise "private" information can be acquired without an intrusive search or seizure. Machine learning can implicate privacy through "category-jumping inferences" that "reveal attributes or conditions an individual has specifically withheld from others."[149] For example, health conditions can be inferred from spending-related information, and behaviors or dispositions can be gleaned from health-related data.[150]

The availability of machine-learning tools means that a determined restrictionist prosecutor or civil plaintiff does not need to depend merely on the data trails left by a pregnant person's deliberate search for abortion care. At least in theory, they can mine large pools of commercially-produced data to generate a model that estimates the likelihood of a pregnancy using extraneous data about a specific person. Just as Target mined its transactional data, so too the restrictionist actor might try to leverage another large pool of data for predictive ends. This may sound implausible now. But several federal agencies, including the Internal Revenue Service and the Securities and Exchange Commission, have developed bespoke predictive tools to mine governmental and private data in order to identify regulatory violations.[151] Is it so far-fetched to suggest that the state of Texas will be lagging far behind in the creative exploitation of retail or social-media data?[152] Or that it could simply hire someone to perform this service for it?

---

148 Cary Coglianese & Alicia Lai, *Algorithm vs. Algorithm*, 72 DUKE L.J. 1281, 1305–06 (2022) (describing advancements in digital algorithms and machine learning in recent decades); *see also* M.I. Jordan & T.M. Mitchell, *Machine Learning: Trends, Perspectives, and Prospects*, 349 SCIENCE 255, 255 (2015) (focusing on improvements in machine learning algorithms).

149 Eric Horvitz & Deirdre Mulligan, *Data, Privacy, and the Greater Good*, 349 SCIENCE 253, 253 (2015) (describing ways in which machine learning can facilitate inferences about health conditions from non-medical data).

150 Aziz Z. Huq, *Constitutional Rights in the Machine-Learning State*, 105 CORNELL L. REV. 1875, 1929 (2020).

151 DAVID FREEMAN ENGSTROM, DANIEL E. HO, CATHERINE M. SHARKEY & MARIANO-FLORENTINO CUÉLLAR, GOVERNMENT BY ALGORITHM: ARTIFICIAL INTELLIGENCE IN FEDERAL ADMINISTRATIVE AGENCIES 10 (2020), https://law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf [https://perma.cc/G2DX-K39E].

152 Reliance on predictive technologies, moreover, may increase as the public becomes aware that personal data collected by private firms creates a risk of state penalties. Assuming (plausibly) that consumer behavior is somewhat elastic, we would expect to see some people migrating over to applications that did not share, or actively hid, personal data. *See* Niva Elkin-Koren & Michal S. Gal, *The Chilling Effect of Governance-by-Data on Data Markets*, 86 U. CHI. L. REV. 403, 417–18 (2019) (describing indicators of changes in user behavior as a result of law enforcement data surveillance).

* * *

The resulting epistemic context in which new conflicts over abortion will unfurl has a largely bilateral, "mirrored" structure. On the one hand are the efforts by patients to access information and then services in ways that ordinarily leave data trails. On the other hand are the efforts of restrictionist law enforcement and civil plaintiffs to isolate those digital breadcrumbs as a way of identifying pregnancies or efforts to access reproductive care. Law enforcement can use the data trail to "mirror" the earlier activity of patients—recreating a map of their movements, inquiries, and even thoughts. This sort of mirroring through digital data is not quite perfect—it will have gaps and discontinuities. But it may well be that the state at some point will be able to infer private facts and thoughts without a data trail that mirrors earlier activity. It may be, that is, that machine learning tools become a means to draw inferences about pregnancy from seemingly extrinsic data.

In the digital economy's context, both law enforcement and nongovernmental groups also have access to a variety of forms of compulsory legal process to compel technology companies to hand over any abortion-sensitive data that the companies possess. Law enforcement can compel companies to disclose noncontent data, such as location data, associations data, biometric data, time stamps, and other metadata, using a mere subpoena.[153] They can use search warrants as a way to compel disclosures of the contents of stored electronic communications, such as emails, private messages, and photographs.[154] Meanwhile, nongovernmental groups who simply file a complaint in court will be entitled to use civil subpoena power to compel disclosures of much or all of the same information.[155]

It is against this backdrop that questions about not just firms' ethical and legal obligations, but also strategies for reproductive privacy necessarily arise. And it is to those questions we now turn.

II
The Private Regulation of Digital Privacy After *Dobbs*

The personal data economies through which biometric, communication, location, health, and financial data flow are in the first instance

153 *See* 18 U.S.C. § 2703.

154 *See* Matthew R. Langley, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables*, 103 Geo. L.J. 1641, 1652 (2015) (summarizing legal means for acquiring content and noncontent data).

155 Fed. R. Civ. P. 45.

the result of private firms' decisions about how data is collected, stored, and disseminated. Digital platforms, search firms, and other so-called "big tech" companies make important structural decisions that shape these flows—and that long precede discrete determinations as to whether to release specific caches of data at the request of a restrictionist prosecutor or civil plaintiff.[156] These structural decisions are influenced by law. But they also determine the degrees of freedom both patients and their restrictionist opponents have in securing or dissolving privacy. In addition to legal considerations, big tech's structural decisions will be shaped by market considerations and by the ethical concerns of their customers and employees.

This Part identifies and analyzes the complex legal, commercial, and ethical environment in which these structural choices will be made. Our threshold aim is to demonstrate that firms' efforts to maintain a studied neutrality on abortion-related questions is almost certain to fail. The distinctions that digital platforms try to draw—between employees and users, or between restrictionist and pro-choice jurisdictions—are unlikely to hold up: Both the character of restrictionist state action and the underlying mechanics of personal data economies make those distinctions exceedingly fragile. Building on this positive, descriptive claim, we then offer predictions about firm-level incentives.

We think it is in the interest of many such firms to structure personal data economies to maximize patients' privacy and decisional autonomy, and to minimize the extent of default or costless compliance with restrictionist efforts to secure data. At the limit, there is a difficult question as to whether firms should comply with or disobey legal instructions that their management or owners believe are immoral, although we recognize that this cuts both ways in respect to abortion. We identify powerful reasons for corporations to resist the search efforts respecting reproductive choice by either their employees or their users, and to absorb fiscal and operational costs related to the defense of privacy in so doing.

We begin by exploring the fragility of existing demarcations that firms have set forth—the employee/user line, and the geographic/jurisdictional line. These turn out to be illusory. We then turn to the ethical and legal arguments for resistance to restrictionist mandates and demands. We defer to Part III, however, a close analysis of the

156 "Big tech" is often associated with the GAFA companies—Google, Amazon, Facebook, and Apple. For a sweeping, journalistic account of the rise of these four companies, see SCOTT GALLOWAY, THE FOUR: THE HIDDEN DNA OF AMAZON, APPLE, FACEBOOK, AND GOOGLE (2017).

specific domains in which epistemic access will be contested and a specific taxonomy of privacy-facing corporate actions.

A. Distinguishing Users from Employees

Corporate responses to *Dobbs* have varied from industry to industry. We focus here on the response of digital platforms such as Google, Meta, Amazon, Twitter, Uber, and Lyft. All these platforms act as the major de facto repositories of the digital trails of biometric, communication, and locational data produced by patients and sought by restrictionist actors.[157] These big tech firms are for this reason differently situated, so far as the personal data economy is concerned, from other major corporate entities in the economy that collect, exploit, and sell personal data as a sideline to another business venture.

The uniform response to *Dobbs* among these firms—with only one significant exception—has been to draw a sharp distinction between users and employees. Firms such as Amazon,[158] Meta (Facebook's parent company),[159] and Alphabet (Google's parent company)[160] have committed to paying for employees' travel out of state to obtain reproductive care. Microsoft, for example, declared that it would "do everything [it] can under the law," including paying travel expenses for "lawful medical services" where access to care is "limited in availability in an employee's home geographic region."[161] On the

---

[157] Hence, we do not address here entities covered by the HIPAA Privacy Rule or financial entities covered by Gramm-Leach-Bliley.

[158] Ike Swetlitz & Spencer Soper, *Amazon, Disney, AT&T Gave to Abortion Foes Like DeSantis While Vowing to Help Employees*, BLOOMBERG (June 30, 2022, 9:05 PM), https://www.bloomberg.com/news/articles/2022-06-30/amazon-disney-at-t-donated-to-desantis-and-other-abortion-opponents#xj4y7vzkg [https://perma.cc/YYG3-8JNA] (describing Amazon's message to staff providing up to $4,000 to cover travel costs for reproductive care).

[159] Abby Ohlheiser & Hana Kiros, *Big Tech Remains Silent on Questions About Data Privacy in Post-*Roe *US*, MIT TECH. REV. (June 28, 2022), https://www.technologyreview.com/2022/06/28/1055044/big-tech-data-privacy-supreme-court-dobbs-abortion [https://perma.cc/2V36-L8ZB].

[160] Jennifer Elias, *Google Memo on End of* Roe v. Wade *Says Employees May Apply to Relocate 'Without Justification*,' CNBC (June 24, 2022, 7:28 PM), https://www.cnbc.com/2022/06/24/google-memo-to-employees-on-roe-v-wade-overturn.html [https://perma.cc/6XN4-J874].

[161] Kyle Wiggers, *Tech Companies Respond to US Supreme Court Abortion Decision*, TECHCRUNCH (June 24, 2022, 12:12 PM), https://techcrunch.com/2022/06/24/tech-companies-respond-to-u-s-supreme-court-abortion-decision [https://perma.cc/FK7P-5CKW]. There is somewhat less to this commitment than might first appear. Firms' commitments to cover travel costs do not extend to "temps, vendors, and contractors—dubbed TVCs," who are less likely to have the independent resources to access reproductive care. Caitlin Harrington, *Tech Companies Will Cover Abortion Travel—but Not for All Workers*, WIRED (July 7, 2022, 7:00 AM), https://www.wired.com/story/tech-

day that *Dobbs* was handed down, Alphabet's Chief People Officer informed all employees that its employees could "apply for relocation without justification, and those overseeing this process will be aware of the situation."[162] Many other companies, including Uber, Lyft, Netflix, Airbnb, Zillow, and Dell, expanded benefits and, in some instances, committed to covering employees' travel expenses in the wake of *Dobbs*.[163] An exception to this trend, as of this writing, appears to be Twitter, which has made no announcement of their policy (if any).[164] In these respects, digital platforms have followed a set of human-resources policies common to many (but by no means all[165]) major corporations in the United States.[166]

But digital giants such as Amazon, Meta, and Alphabet, as well as platforms such as Twitter, are not like other companies. In particular, the former companies do not merely possess personal data that is produced as an incident of a specific commercial transaction. They also have a large pool of personal data that is generated by the search,

---

companies-abortion-travel [https://perma.cc/6GXN-66KX] (describing the responses of Amazon, Google, Uber, Lyft, and DoorDash). Temporary workers comprise a larger share of the Google workforce than full-time employees as of 2019. Daisuke Wakabayashi, *Google's Shadow Work Force: Temps Who Outnumber Full-Time Employees*, N.Y. TIMES (May 28, 2019), https://www.nytimes.com/2019/05/28/technology/google-temp-workers.html [https://perma.cc/4NC4-J8X4].

162 Elias, *supra* note 160. It would be ironic if employees had to disclose both their pregnancy and their intention to seek an abortion in order to avail themselves of this option. As we read statements such as Alphabet's, however, no such disclosures are entailed. The more sensible policy, in any event, would not elicit or record the reasons for a move.

163 *See Companies with Extended Women's Health Benefits*, YALE SCH. MGMT. CHIEF EXEC. LEADERSHIP INST., https://mk114283.wixsite.com/website [https://perma.cc/F8SD-Z68C] (summarizing companies' updated health policies and sources for new benefits).

164 *See* Wiggers, *supra* note 161. It seems likely that the firm's purchase by Elon Musk and the ensuing changes to staffing and policy will consume its attention—assuming, that is, the platform survives with anything like its former model.

165 Other entities such as law firms have been more cautious to date even in taking a position on the provision of reproductive care to their employees. Meghan Tribe & Maia Spoto, *Big Law Mostly Quiet on Abortion Aid as Texas Battle Rages*, BLOOMBERG L. (July 15, 2022, 6:29 PM), https://news.bloomberglaw.com/business-and-practice/big-law-mostly-quiet-on-abortion-aid-as-texas-battle-rages [https://perma.cc/9U6Y-WTX6] ("Roughly two-thirds of the 70 largest law firms with Texas offices have not publicly said whether they will cover employees' costs to travel for abortions . . . .").

166 *See* David Shepardson & Dawn Chmielewski, *Disney, Other U.S. Companies Offer Abortion Travel Benefit After* Roe *Decision*, REUTERS (June 25, 2022, 10:10 AM), https://www.reuters.com/world/us/disney-other-us-companies-offer-abortion-travel-benefit-supreme-court-strikes-2022-06-24 [https://perma.cc/L9Z9-UTGK] (listing companies' travel benefits post-*Dobbs*, including Disney, Alaska Air Group, JPMorgan, and Dick's Sporting Goods); Claire Duffy & Jennifer Korn, *These US Companies Will Cover Travel Costs for Employees Who Need an Abortion*, CNN BUSINESS (June 27, 2022, 2:34 PM), https://www.cnn.com/2022/06/24/tech/companies-abortion-reaction/index.html [https://perma.cc/3QLC-M4PB] (summarizing policies of U.S. companies in response to *Dobbs*).

movement, and actions of their users. The difference, we emphasize, is one of scale rather than kind. Many firms that are not thought of as part of the digital economy also aggregate a large volume of personal data about their customers: Think about automobile manufacturers, or those who make "smart" fridges and stoves. But such data tends to train on a relatively narrow set of transactions between the customer and the firm.[167] In contrast, big tech has a wider and more detailed data-based perspective on their users. Their "entire business model[] [is] built on selling and monetizing data" in a way that other firms' are not.[168] Further, the patient-search activities detailed in Section I.A will often leave big tech (but not other entities) digital traces that facilitate relatively direct inferences about reproductive health choices. In contrast, other firms' data may reveal such choices—but only indirectly. Extracting them may well require costly and technically complex analytic methods.

In stark contrast to its solicitude about employees, big tech has demonstrated very little concern about the novel exposure of its users to civil and criminal liability. In general, these same digital platforms have declined to respond to media queries concerning their post-*Dobbs* policies in respect to law enforcement requests for data.[169] Exceptions run in both directions. On the one hand, Meta has promulgated a policy that prohibits its employees from posting about *Dobbs*, despite the firm's financial support for employee access to reproductive care.[170] On the other hand, Google announced in July 2022 that it would automatically delete from the Google Location History entities such as "counseling centers, domestic violence shelters, abortion clinics, fertility centers, addiction treatment facilities, weight loss clinics, cosmetic surgery clinics, and others . . . soon after they visit."[171]

---

[167] For a discussion focused on one such industry, see James McCandless, *Privacy Concerns Aren't Keeping Automakers from Selling Massive Amounts of Your Data*, NEWSWEEK (Oct. 27, 2021, 12:02 PM), https://www.newsweek.com/privacy-concerns-arent-keeping-automakers-selling-massive-amounts-your-data-1634478 [https://perma.cc/AX7N-WSXX] (reporting on car manufacturers' practices of collecting driver data).

[168] RANA FOROOHAR, DON'T BE EVIL: THE CASE AGAINST BIG TECH 19 (2019) (comparing data collecting practices of big tech versus other companies).

[169] *See, e.g.*, Ohlheiser & Kiros, *supra* note 159 (reporting that Alphabet, Reddit, TikTok, and Meta declined to respond to MIT Technology Review's requests for information on how the companies would respond to abortion-related data requests from law enforcement).

[170] Maxwell Newman, *Meta Forbids Workers from Discussing Abortion Ruling*, NEWSMAX FINANCE (July 5, 2022, 4:18 PM), https://www.newsmax.com/finance/streettalk/meta-abortion-dobbs-v-jackson-womens-health-supreme-court/2022/07/05/id/1077435 [https://perma.cc/BX6U-HE3P].

[171] Jen Fitzpatrick, *Protecting People's Privacy on Health Topics*, THE KEYWORD: GOOGLE BLOG (July 1, 2022), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics [https://perma.cc/BGJ6-RR5C].

And the period tracking app Flo announced that it would offer an "Anonymous Mode" for users.[172] In contrast, many other pregnancy related apps make it difficult, or perhaps even impossible, to opt out of sharing personal data.[173]

Google's July 2022 announcement about locational data is, at the time of our writing at least, the sole significant move by big tech aimed at protecting users, as well as employees, from restrictionist uses of the law. The balance of firms at the heart of the personal data economy have settled on a sharp distinction between employers and users: The former will be offered financial support, and perhaps relocation expenses, to facilitate reproductive choice. The latter will not be protected at all.[174]

But this line between users and employees is not stable or tenable. Although it seems to have been an attractive compromise for technology firms in the immediate aftermath of *Dobbs*, it is likely to collapse. This will be to the detriment of employees, who will find that their reproductive choice set is thereby dramatically undermined.

A threshold problem is that the distinction rests upon the implausible assumption that employees are not also users, and that they cannot be targeted as users if they dare to exercise their job-related entitlements. Those who work for Google or Facebook also probably use their products. As a result, they would likely leave data trails if they accessed reproductive care. Under the policies adopted by these firms (with the exception of that of Google as to locational data),

---

172 Alan Martin, *Period-Tracking Apps Respond to* Roe v. Wade *Ruling*, TOM'S GUIDE (Aug. 25, 2022), https://www.tomsguide.com/news/period-tracking-apps-respond-to-roe-v-wade-ruling [https://perma.cc/XS3M-HUK5]. Curiously, another app, Clue, responded by averring that they would follow European privacy rules—which also allow disclosures to law enforcement. *Id.*

173 Veronica Barassi, *BabyVeillance? Expecting Parents, Online Surveillance and the Cultural Specificity of Pregnancy Apps*, 3 SOC. MEDIA + SOC'Y 1, 6 (2017) (finding "a great level of ambiguity with reference to users' possibility to opt out" in the terms of service of many pregnancy-related apps); *see also* Nazanin Andalibi, *Symbolic Annihilation Through Design: Pregnancy Loss in Pregnancy-Related Mobile Apps*, 23 NEW MEDIA & SOC'Y 613, 619 (2021); Barassi *supra*, at 6 (reporting ethnographic evidence that users found opt-out hard to manage). Other pregnancy related apps use "gamification" strategies that make it more costly to exit the app. Gareth M. Thomas & Deborah Lupton, *Threats and Thrills: Pregnancy Apps, Risk and Consumption*, 17 HEALTH, RISK & SOC'Y 495, 495–97 (2015) (discussing these "ludification" strategies).

174 For a pessimistic prediction, see Natasha Singer & Brian X. Chen, *In a Post-*Roe *World, the Future of Digital Privacy Looks Even Grimmer*, N.Y. TIMES (July 13, 2022), https://www.nytimes.com/2022/07/13/technology/personaltech/abortion-privacy-roe-surveillance.html [https://perma.cc/H4JF-7S77] ("The tech giants that control how our data is collected—the same ones that have professed for years in marketing campaigns that they care about privacy—have not made plans to substantially change the way they hoover up information.").

restrictionist prosecutors could use warrants or subpoenas to obtain data on a firm's employees.

Hence, imagine a digital firm that offers its employees financial support to obtain reproductive care but takes none of the steps identified in Part III to protect its users' privacy. Indeed, there is a perverse incentive for a restrictionist prosecutor to target those employees as a way of gaining leverage over the firm as a whole. That is, it would be straightforward for restrictionist law enforcement to secure the personal data of the firm's employees in order to bring actions against those who reside in a jurisdiction where abortion is criminalized but travel outside the state to secure care. Law enforcement would simply obtain, by compulsory process or otherwise, locational data linking the firm's offices to abortion providers. Just by threatening to do so, the prosecutor might aim to pressure the firm into more general forms of cooperation. The mere specter of disruption to the workplace may be enough to induce the firm's compliance. Alternatively, law enforcement could even bring actions against employees who reside in nonrestrictionist states. To be sure, such actions would be more difficult to bring as a result of jurisdictional limitations under the Due Process Clause if an employee is not located in a restrictionist state.[175] But as we explore below, it would be premature to conclude that restrictionist efforts to squelch abortions will stop at state lines. It suffices here to say that even if an employee does not reside or work in a restrictionist state, we think that it is hardly impossible for a sufficiently determined law enforcement entity or civil plaintiff to seek out a means to have them arrested or sued. And we anticipate that they will have plenty of reasons to do so.

To be sure, it is likely that a disproportionate number of big tech employees have the knowledge and capacity (in terms of technical understanding of operating systems) to maximize privacy and minimize state collection of their own or their loved ones' data trails. But it is important to recognize that this would not eliminate all litigation risk for big tech's employees. Some might enter the market for reproductive care after a period of being unknowingly pregnant or a period of being knowingly and publicly pregnant. It is common now to post images from a pregnancy, including sonogram photographs, on social media platforms.[176] The pregnant trade medication advice and "regularly post images of books, magazines, and screen-grabs of their preg-

---

175 *See infra* Section II.B.

176 Tama Leaver & Tim Highfield, *Visualizing the Ends of Identity: Pre-birth and Post-death on Instagram*, 21 INFO., COMMC'N & SOC'Y 30, 36 (2016) (finding 11,320 images and videos hashtagged #ultrasound between March and May 2014).

nancy apps."[177] Where the pregnancy subsequently endangers the mother's health—an eventuality that does not make access to abortion legal in several states[178]—they may choose to seek termination to protect their own health or life. An assumption that employees will be technologically sophisticated enough to protect themselves has the untoward effect of omitting those who face the most serious health consequences from pregnancy and who have been candid about their pregnancies.[179]

A second and related problem is that restrictionist prosecutors can leverage the vulnerability of employees to prosecution in order to pressure firms to withdraw that protection. That is, they can adopt policies and structural choices that extend the scope of or facilitate the operation of, restrictionist regimes to cover a firm's operation—for example by threatening firms that have in-state operations for the policies of their out-of-state offices. The very fact that a firm has privileged, asymmetrical access to the data traces that facilitate prosecutorial searches may well create an incentive for restrictionist actors to seek out and use legal tools against those firms' employees. For even if firms are located largely outside a restrictionist jurisdiction, there is a possibility that an officer or employee of the firm will be exposed to prosecution or civil action because of actions taken by the entity as a whole.

We analyze further the dynamics of extraterritoriality in the following Section—which considers, and rejects, the feasibility of geographic distinctions with respect to the handling of data. But it is worth briefly anticipating that discussion with a single example: Within weeks of *Dobbs* being handed down, Texas politicians had threatened partners of the law firm Sidley Austin with criminal prosecutions if they funded reproductive care prohibited in Texas.[180] Most of the Sidley partners, of course, were not located in Texas, and it was not clear whether the threat applied to Sidley employees in Texas alone. It also remains unclear as of this writing whether any prosecutor in the state has any real intention to secure an indictment

---

[177] Katrin Tiidenberg & Nancy K. Baym, *Learn It, Buy It, Work It: Intensive Pregnancy on Instagram*, 3 SOC. MEDIA + SOC'Y 1, 4 (2017).

[178] *See supra* text accompanying notes 9–14.

[179] Alternatively, the pregnant could choose to withhold news about their condition online in order to maintain their option to secure reproductive care, should a need arise. This seems implausibly psychologically demanding—as it assumes that the pregnant will behave out of a consciousness for the worst-case scenario.

[180] Weiss, *supra* note 6.

against either Sidley or another law firm that facilitates its employees' reproductive choice.[181]

The rather obvious point of such a public threat against a prominent law firm, of course, was (and is) to achieve an *in terrorem* effect—scaring not just Sidley but other corporate entities into withholding funds to facilitate their employees' reproductive choice. The incident shows how the mere threat of criminal penalties against an employee can be used (and has been used) to obtain leverage against a company operating largely outside the relevant state—and how restrictionist states are perfectly willing to flex their criminal and civil powers to this end.

How else might this occur in practice? A restrictionist state could threaten to target for investigation and prosecution the employees of an ISP or a social network in order to prevent it from offering insurance coverage for reproductive care, or (more likely) as a way to secure "voluntary" compliance with aggressive demands for digital information that would advance more generally restrictionist goals. This would not require data from the ISP or social network in the first instance. Even without that, law enforcement could seek a geofence warrant that covers the geographic area for the reproductive health facilities near the company.[182] Note that law enforcement could obtain such a warrant at present from a home-state court even if the ISP or digital platform was not located within their jurisdiction.[183] Law enforcement would then hone in upon those employees seeking care. It could threaten to bring suit against them, once again as a means to leverage greater compliance or even positive assistance beyond the requirements of the law from the ISP or digital platform.

In sum, the distinction between employees and users is a hollow one. Unless employees are protected as users, they will be vulnerable to prosecution. Indeed, the very fact that they are employed by an entity that has an asymmetrical access to or control over personal data makes them a tempting target for investigation or prosecution. Even if

---

[181] Note how broadly this threat runs: Imagine that a Sidley associate seeks a transfer between offices and then happens to have an abortion. Would the fact of permitting the transfer, knowing that the associate is pregnant, be enough for criminal liability? Would the firm have a duty to ask the associate? Could the associate be terminated if she declined to answer? Could the firm access the associate's medical records to determine whether she could be pregnant? The list of questions goes on.

[182] *See supra* notes 97–99 and accompanying text.

[183] *See* Lozoya v. State, No. 07-12-00142-CR, 2013 WL 708489 (Tex. Crim. App. Feb. 27, 2013) (upholding the issuance of a search warrant by a Texas trial court for cell phone records held in Overland Park, Kansas); *see also* State v. Esarey, 67 A.3d 1001, 1008 (Conn. 2013) (permitting the issuance of a search warrant for electronic records held extraterritorially, noting the appropriateness of such a decision where there is a likelihood that such records would not be held within the state).

the distinctive treatment of employees is a plausible solution for non-tech companies, it is very likely to be an unstable equilibrium when it comes to big tech.[184] To be clear, we do not claim that tech companies ought to cease to facilitate relocation and otherwise support pregnant employees. Rather, we think this is unlikely to be a sufficient response.

B. Drawing Geographic Lines

Tech firms may be tempted to draw a second sort of distinction to manage the post-*Dobbs* dispensation: They might be attracted to the idea that they will comply with restrictionist laws, and efforts to enforce them, that arise within a state that criminalizes abortion, but not do so outside such a state. Policies to the effect that employees' travel to another state or permanent relocation from a restrictionist location will be funded or enabled already nod toward this possibility: In effect, they declare, firms will comply with the law within the geographic boundaries in which that law is supposed to apply.

A geographic distinction, however, is doomed to falter just as much as an employee/user distinction. First, the movement of pregnant bodies across borders means that regulation will not be geographically limited. Second, restrictionist efforts to apply primary rules of conduct through civil and criminal law are not and will not be limited to states in which abortion is prohibited. Third, restrictionist efforts to gather information are not limited by law to their own state borders. Finally, the personal data economy cannot be easily geographically segmented within the United States; it does not lend itself to partition between restrictionist and non-restrictionist domains. The net result of these legal and technological factors is that any effort by tech firms to establish geographic bounds on compliance with restrictionist enforcement efforts is likely to flounder. To see why geography supplies no limiting principle, we can consider each of these points in turn.

---

[184] We have focused here on the dynamics created by state prosecution efforts. We note that federal agencies also have the ability to leverage regulatory authorities to "create effective regulatory power that it would not otherwise possess," including access to data that would otherwise require a warrant to obtain, or that otherwise would not be collected. Daphna Renan, *Pooling Powers*, 115 COLUM. L. REV. 211, 214 (2015). We leave to another day questions about the ways in which regulatory tools in the federal government's arsenal could be deployed to restrictionist ends, even without a change to the substance of federal criminal law, but flag their importance here.

1. Patient Search Across Borders

As an initial matter, a pregnant body is not confined to one state. Restrictionist regimes, indeed, create powerful incentives for those seeking medical care to cross state lines in search of treatment. This dynamic emerged before *Roe*. The deregulation of abortion occurred first at the state level at the end of the 1960s.[185] In July 1970, New York State legalized abortions up to twenty-four weeks. In the following two years, one study identified 334,865 abortions performed in the state, out of which 220,163 (or 65.7%) involved non-residents.[186] Although data are sparse, it seems likely that this flow of bodies continued in the years after *Roe* as a consequence of a persistent and strong local resistance to abortion.[187] Today, residents in states with more restrictive laws still move across state lines to obtain care. For example, in 2020, only 167 abortions were performed in Missouri, while 3,201 Missouri residents received such care in Kansas in the same year.[188] Some patients are airlifted across state lines to avoid abortion bans.[189] In the immediate weeks after *Dobbs*, national attention congealed around a ten-year-old girl who had been raped and then crossed state lines from Ohio to Indiana to abort a pregnancy.[190] That story further confirmed that the flow of bodies across state lines had continued despite *Dobbs*.

---

185 GERALD N. ROSENBERG, THE HOLLOW HOPE: CAN COURTS BRING ABOUT SOCIAL CHANGE? 183–84 (2d ed. 2008).

186 Jean Pakter, Donna O'Hare, Frieda Nelson & Martin Svigir, *Two Years Experience in New York City with the Liberalized Abortion Law—Progress and Problems*, 63 AM. J. PUB. HEALTH 524, 524 (1973).

187 *See* ROSENBERG, *supra* note 185, at 189–94 (finding that many hospitals refused to perform abortions, requiring over 150,000 women to travel out of state for abortion services in 1973 and 100,000 women to do the same in 1982).

188 Josh Merchant, *Nearly Half of Abortions in Kansas Are for Missourians. A Vote Next Year Could Change That*, MO. INDEP. (Nov. 22, 2021, 1:00 PM) https://missouriindependent.com/2021/11/22/nearly-half-of-abortions-in-kansas-are-for-missourians-a-vote-next-year-could-change-that [https://perma.cc/5VHA-QJFL].

189 Tessa Stuart, *Pilots Are Airlifting Patients Out of Red States to Get Abortions*, ROLLING STONE (June 29, 2022) https://www.rollingstone.com/politics/politics-features/elevated-access-volunteer-pilots-abortion-1375732 [https://perma.cc/4ZWR-Y6ER] (reporting that a nonprofit called Elevated Access was formed to fly persons in need of abortion or gender affirming care to states where they can access those services).

190 *See* Katie Robertson, *Facts Were Sparse on an Abortion Case. But That Didn't Stop the Attacks*, N.Y. TIMES (July 14, 2022) https://www.nytimes.com/2022/07/14/business/media/10-year-old-girl-ohio-rape.html [https://perma.cc/4GT3-6NXM] (reporting on the extent to which the case captured national media attention). The case led to a threat of prosecution against the Indiana provider. Alice Miranda Ollstein, *Indiana AG Eyes Criminal Prosecution of 10-year-old Rape Victim's Abortion Doc*, POLITICO (July 14, 2022) https://www.politico.com/news/2022/07/14/indiana-abortion-rape-ohio-00045899 [https://perma.cc/V2ZQ-34FU].

In addition to the physical movement of bodies, abortion regulation will motivate an uptick in digital and physical searches for medical care across borders. Even before the COVID-19 pandemic, medication abortion constituted some forty-eight percent of abortions provided in the United States.[191] This was at a time when patients had to attend an in-person consultation to receive medication. In December 2021, however, the FDA allowed the abortifacient mifepristone to be prescribed remotely and without an in-person pick-up from a certified provider.[192] As a result, abortion became "untethered to a clinical space,"[193] at least in the absence of a state-law requirement of in-person prescription.[194] Even where state law prohibits the remote prescription of mifepristone,[195] overseas nonprofits such as Aid Access offer remote abortion to patients within the first ten weeks of a pregnancy at a cost of $105.[196] Even if the FDA reimposes an in-person consultation requirement, it seems likely that patients will still search for, and often be able to find, abortion medication online. Due to the wide diffusion of providers, this will again render state-based distinctions untenable.

---

191 Katherine Kortsmit, Antoinette T. Nyugen, Michele G. Mandel, Elizabeth Clark, Lisa M. Hollier, Jossica Rodenhizer & Maura K. Whiteman, *Abortion Surveillance—United States, 2019*, MORBIDITY & MORTALITY WKLY. REP., Nov. 26, 2021, at 6, https://www.cdc.gov/mmwr/volumes/70/ss/pdfs/ss7009a1-H.pdf [https://perma.cc/E7HK-BWDS] (citing the percentage of abortions that were medical abortions at 7–9 weeks gestation).

192 The regulatory change, as we have noted, was a response to the COVID-19 pandemic. *See* Recent Guidance, *Reproductive Rights–Medication Abortion–FDA Lifts In-Person Dispensing Requirement for Mifepristone Abortion Pill–Update to FDA's Risk Evaluation and Mitigation Strategy for Mifepristone on Dec. 16, 2021, Eliminating In-Person Dispensing Requirement*, 135 HARV. L. REV. 2235, 2236–37 (2022) (discussing the shift in the legal regime prompted by the FDA's new Mifepristone REMS Program); U.S. FOOD & DRUG ADMIN., RISK EVALUATION AND MITIGATION STRATEGY (REMS) SINGLE SHARED SYSTEM FOR MIFEPRISTONE 200MG (2021). The FDA announced the change by updating Question 5 on the webpage *Questions and Answers on Mifeprex*, U.S. FOOD & DRUG ADMIN. (Dec. 16, 2021), https://www.fda.gov/drugs/postmarket-drug-safety-information-patients-and-providers/questions-and-answers-mifeprex [https://perma.cc/QP4M-Y3FG] (stating that the agency had removed the in-person dispensing requirement from the Mifepristone REMS Program).

193 David S. Cohen, Greer Donley & Rachel Rebouché, *The New Abortion Battleground*, 123 COLUM. L. REV. 1, 15 (2023).

194 *See State Laws and Policies: Medication Abortion*, GUTTMACHER INST. (Dec. 1, 2022), https://www.guttmacher.org/state-policy/explore/medication-abortion [https://perma.cc/X7U5-Z466] (identifying 18 states with such a requirement).

195 For an analysis of state-by-state differences on this score, see Sydney Calkin, *Legal Geographies of Medication Abortion in the USA*, 47 TRANSACTIONS OF THE INST. OF BRIT. GEOGRAPHERS 378 (2022).

196 *Consultation*, AIDACCESS, https://aidaccess.org/en/i-need-an-abortion [https://perma.cc/65WD-PED6].

2. *Extraterritorial Criminalization of Abortion*

Just as patient search takes on new, cross-state forms, so too restrictionist states can and will endeavor to prevent medical care from being delivered to their residents in other states. These efforts will take the form of both civil and criminal laws. In 2021, for example, Texas enacted a statute that toughened criminal penalties for remotely prescribing and mailing abortion medication to include jail time and a hefty fine.[197] The bill was praised by its supporters as an effort to reach people "outside of the state's strict limits."[198] At the time of this writing, the colorable risk of indictment and prosecution seems to be limited to instances in which the person seeking reproductive care has at some point been within the jurisdiction of a state that criminalizes abortion.[199] But consider the possibility of a state pursuing prosecutions of pregnant persons who passed through its territory (say, while flying between two other states) and then later obtained an abortion.

Even under this regime, however, substantial uncertainty remains about who would be covered by the prohibition and about the risk of cross-border prosecutions. Consider the case of Missouri. Its criminal code provides that "no abortion shall be performed or induced upon a woman, except in cases of medical emergency."[200] The statute does not define, however, which abortions fall within its coverage. So it leaves open the question whether a procedure performed outside the state on a Missouri resident falls within its reach.[201] Missouri courts, moreover, have "hesitate[d] to essay any definition of 'residence,' for the word is like a slippery eel, and the definition which fits one situa-

---

197 Ashley Lopez, *Prescribing Abortion Pills Online or Mailing Them in Texas Can Now Land You in Jail*, NPR (Dec. 6, 2021), https://www.npr.org/sections/health-shots/2021/12/06/1060160624/prescribing-abortion-pills-online-or-mailing-them-in-texas-can-now-land-you-in-jail [https://perma.cc/4KFY-CWX8].

198 *Id.*

199 For discussion of trends in state-level prosecutions, see Caroline Kitchener, *Conservatives Complain Abortion Bans Not Enforced, Want Jail Time for Pill 'Trafficking'*, WASH. POST (Dec. 14, 2022), https://www.washingtonpost.com/politics/2022/12/14/abortion-pills-bans-dobbs-roe [https://perma.cc/2L67-SLPX] (discussing post-*Dobbs* patterns in prosecution).

200 MO. REV. STAT. § 188.017 (2022).

201 This is not the only facet of Missouri's abortion ban that is deeply ambiguous. *See* Summer Ballentine, *Missouri's Answer to Abortion Law Questions: Don't Ask Us*, ASSOC. PRESS (July 13, 2022), https://apnews.com/article/abortion-health-missouri-columbia-fef01a409b24991a4e56cc70c874f0bd [https://perma.cc/W7XN-7VE3] (detailing how haphazard legal guidance has sown confusion among healthcare providers on what medical care, including some forms of contraception, is prohibited by the state's expansive law).

tion will wriggle out of our hands when used in another context or in a different sense."[202]

The same dynamic can be observed in the civil law domain. Under Texas's S.B.8, by way of example, "damages in an amount of not less than $10,000 for each abortion" are available against not only anyone who "performs or induces" a covered abortion, but also anyone who "aids or abets the performance or inducement of an abortion, including paying . . . through insurance or otherwise" and without regard to whether "the person knew or should have known that the abortion would be performed or induced."[203] The statute does not contain a geographic limitation. As a consequence, plaintiffs do not need to reside within the relevant jurisdiction. The first suits under S.B.8 were filed by out-of-state plaintiffs against a Texas physician who had written publicly that he had performed a covered procedure.[204] There is no reason, as a matter of statutory construction,[205] to think that S.B.8 could not be invoked against an out-of-state defendant, as well as by an out-of-state plaintiff.

There are a series of difficult and disputed constitutional questions about the scope of a state's power to impose criminal or civil liability on actions that occur outside its borders. In neither case can it be said that the Constitution imposes an iron-clad barrier on the extraterritorial reach of restrictionist measures. Hence, in a recent treatment of questions arising out of the extraterritorial application of state criminal law, Professors David S. Cohen, Greer Donley, and Rachel Rebouché conclude that the "constitutional doctrines related to extraterritoriality are notoriously underdeveloped," throwing up conflicts between "competing fundamental constitutional principles."[206] While there is precedent for the idea that a state "obviously" could not criminalize abortion in another jurisdiction or "prosecute [its residents] for going there,"[207] it remains to be seen whether that

---

[202] State v. Tustin, 322 S.W.2d 179, 180 (Mo. Ct. App. 1959), *abrogated by* State *ex rel.* Dalton v. Riss & Co., 335 S.W.2d 118, 129 (Mo. 1960) (en banc).

[203] Texas Heartbeat Act, S.B.8, 87th Leg., Reg. Sess. (Tex. 2021) (codified at TEX. HEALTH & SAFETY CODE ANN. §§ 171.208(a)(1)–(2) (West 2021)).

[204] Reese Oxnor, *Texas Doctor Who Admitted to Violating the State's Near-Total Abortion Ban Sued Under New Law*, TEX. TRIB. (Sept. 20, 2021), https://www.texastribune.org/2021/09/20/texas-abortion-ban-doctor-alan-braid [https://perma.cc/J8FT-A846].

[205] *See infra* text accompanying notes 209–23 (discussing constraints under the Due Process Clause).

[206] Cohen, Donley & Rebouché, *supra* note 193, at 29, 32.

[207] Bigelow v. Virginia, 421 U.S. 809, 823–24 (1975). For subsequent judicial recognition of the constitutional difficulties presented by the extraterritorial application of criminal law, see, for example, State v. Rimmer, 877 N.W.2d 652, 665–66 (Iowa 2016) ("We agree with the New Jersey Supreme Court that '[t]he extraterritorial application of state criminal

principle survives a Supreme Court openly hostile to reproductive choice and eager to facilitate restrictionist efforts.

In contrast to the uncertainty around extraterritorial criminal liability, the state's power to impose tort liability through measures such as S.B.8 is certainly "not extinguished by the fact that the tortfeasor is a nonresident. State long-arm statutes exist to vindicate the state's own interests when the tortfeasor is a nonresident."[208] To be sure, the Due Process Clause imposes some limits on the reach of a state's civil courts.[209] But personal jurisdiction doctrine under the Due Process Clause will often allow a civil suit against an individual (or firm) located outside the restrictionist state. Current constitutional doctrine distinguishes between exercises of general and specific jurisdiction for Due Process purposes. "A state court may exercise general jurisdiction only when a defendant is 'essentially at home' in the State."[210] The resulting grant of jurisdiction allows for claims that "concern events and conduct anywhere in the world."[211] For a corporate defendant, general jurisdiction exists in the place of incorporation and the principal place of business.[212] In contrast, specific jurisdiction obtains where an individual or corporate defendant "purposefully avails itself of the privilege of conducting activities within the forum State."[213]

---

law is subject to due process analysis' under the Fourteenth Amendment.") (quoting State v. Sumulikoski, 110 A.3d 856, 866 (N.J. 2015)); State v. Randle, 647 N.W.2d 324, 329 n.4 (Wis. Ct. App. 2002) ("Territorial jurisdiction is part of the due process restrictions on the power of a court . . . .").

208 Louise Weinberg, *Sovereign Immunity and Interstate Government Tort*, 54 U. MICH. J.L. REFORM 1, 55 (2020).

209 Cohen, Donley, and Rebouché's excellent and meticulous article focuses primarily on criminal rather than civil liability. *See* Cohen et al., *supra* note 193, at 31–34. We hence detail the latter more closely.

210 Ford Motor Co. v. Montana Eighth Jud. Dist. Ct., 141 S. Ct. 1017, 1020 (2021) (quoting Goodyear Dunlop Tires Operations, S.A. v. Brown, 564 U.S. 915, 919 (2011)).

211 *Ford Motor*, 141 S. Ct. at 1024. This is a narrower version of general jurisdiction than historically has been used. In *Daimler AG v. Bauman*, the Court rejected as "unacceptably grasping" the longstanding understanding that a "substantial, continuous, and systematic course of business" supported general jurisdiction. Daimler AG v. Bauman, 571 U.S. 117, 138 (2014).

212 *Ford Motor*, 141 S. Ct. at 1024. *Ford* marked a recession from an earlier account of general jurisdiction that was "not limited" to those cases including instances in which "corporate defendant's operations in another forum 'may be so substantial and of such a nature as to render the corporation at home in that State.'" BNSF Ry. Co. v. Tyrrell, 581 U.S. 402, 414 (2017) (quoting *Daimler AG*, 571 U.S. at 139 n.19); Goodyear Dunlop Tires Operations, S.A. v. Brown, 564 U.S. 915, 919 (2011) (stating that a state court may assert general jurisdiction over a corporation domiciled in another state when the corporation's connections to the state are so "continuous and systematic" that they make the corporation "essentially at home in the forum State"). One (unintended?) consequence of *Ford* is that corporate defendants in S.B.8-type actions can be sued in far fewer courthouses around the country.

213 Hanson v. Denckla, 357 U.S. 235, 253 (1958); *accord Ford Motor*, 141 S. Ct. at 1024.

The application of these rules in practice presents complex questions. Imagine, for example, that a digital platform is sued in its state of incorporation using S.B.8's cause of action. Both Alphabet and Meta are incorporated in Delaware. Whether the suit could proceed then would depend on a complex set of choice of law, choice of forum, and forum non conveniens doctrine.[214] The resulting uncertainty, however, may well chill individual providers and firms alike.[215]

Even if restrictionist efforts focus on residents of their own states, their natural (and perhaps intended) effect will be to restrict the availability of medical care for residents of other states. Prior to *Roe*, physicians in states where abortion was lawful refused requests to provide medical care "because of the specter of legal liability."[216] Ambiguity about the scope of criminal liability—for example, because of uncertainty as to who counts as a "resident"—means that in the short term at least, risk-averse providers are faced with difficult questions of how to screen potential patients for criminal liability exposure. It is not hard to imagine how this sort of litigation uncertainty could lead to a dramatic decline in the provision of abortion nationwide, especially among clinics located close to states with abortion prohibitions.

3. Extraterritorial Investigations

In Part I, we briefly canvassed the range of tools, from administrative subpoenas to warrants, that could be used to obtain personal data showing patients' search efforts. Just as enforcement can spill over state borders, so too can efforts to gather such data. If states want to prevent their residents from seeking reproductive care across a state border, it is almost inevitable that they will seek records that are physically located across state lines. At present, there are few legal barriers to the use of compulsory legal process as a means of eliciting the disclosure of such evidence. Instead, its collection and use depend upon the procedural mechanisms available to law enforcement and civil litigants for securing out-of-state evidence.

The legal framework for between-state requests for information is complex. States have not all adopted a single, uniform statutory

---

[214] For a recent analysis of the latter under Delaware law, see *Aranda v. Philip Morris USA Inc.*, 183 A.3d 1245, 1255 (Del. 2018) (holding that "[a]n available alternative forum is not a threshold requirement before dismissing a case for *forum non conveniens*," but is "a factor to be considered").

[215] The general idea that "litigation uncertainty" can "chill[]" business activity is a familiar one, *see* Robert G. Bone, *Taking the Confusion Out of "Likelihood of Confusion": Toward a More Sensible Approach to Trademark Infringement*, 106 Nw. U. L. Rev. 1307, 1308 (2012), even if its application here is new.

[216] Mary Ziegler, Abortion and the Law in America: *Roe v. Wade* to the Present 11 (2020).

scheme. Nevertheless, a few generalizations are warranted. To begin with, there is no general prohibition on a state invoking the jurisdiction of another state's courts for the purpose of gathering evidence for a criminal matter.[217] Most states have codified a version of the Uniform Act to Secure the Attendance of Witnesses from Without a State in Criminal Proceedings,[218] which allows a prosecutor to obtain an out-of-state court order for a witness to appear or to produce documents.[219] The ensuing state laws generally require that a court in the recipient's state review the out-of-state legal process and issue a local order to enforce it.[220] Similarly, the Uniform Interstate Depositions and Discovery Act (UIDDA) facilitates evidence gathering across state lines in civil cases.[221] It has been adopted in some form by thirty-seven states by one recent count.[222] States adopting the UIDDA allow litigants to use a subpoena issued by a court in the requesting state to obtain discoverable materials from another state that has adopted the UIDDA.[223]

States may also explicitly authorize the execution of out-of-state search warrants for electronically stored information. Under California law, to offer a pertinent example, a corporation located in California "that provides electronic communication services or remote computing services to the general public" must comply with "a warrant issued by another state to produce records . . . as if that warrant

---

[217] *See* Carleen Zubrzycki, *The Abortion Interoperability Trap*, 132 YALE L.J. 197, 197–200 (2022) (discussing the practice). States cannot, however, be sued without their consent in another state's courts. Franchise Tax Bd. of Cal. v. Hyatt, 139 S. Ct. 1485, 1490 (2019).

[218] UNIF. ACT TO SECURE THE ATTENDANCE OF WITNESSES FROM WITHOUT A STATE IN CRIM. PROC. (UNIF. L. COMM'N 1936); *see* Darrell E. White II, *Subpoenaing Out-of-State Witnesses in Criminal Proceedings: A Step-by-Step Guide*, NAT'L ASS'N OF ATT'YS GENS. (May 18, 2021), https://www.naag.org/attorney-general-journal/subpoenaing-out-of-state-witnesses [https://perma.cc/KCX4-XAYD].

[219] Barber v. Page, 390 U.S. 719, 723 n.4 (1968) ("For witnesses not in prison, the Uniform Act . . . provides a means by which prosecuting authorities from one State can obtain an order from a court in the State where the witness is found directing the witness to appear in court in the first State to testify.").

[220] *See* White II, *supra* note 218 (noting that states may require slightly different procedures, but that a prosecutor in State A generally may file a certificate order with a State B court, and that the State B court may issue a summons ordering a witness residing in State B to appear in State A).

[221] *See* UNIF. INTERSTATE DEPOSITIONS & DISCOVERIES ACT, § 3–9 (UNIF. L. COMM'N 2007) (providing for interstate issuance and service of subpoenas, depositions, and production of evidence).

[222] Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687, 693 (2017).

[223] *Id.* at 693–94.

had been issued by a California court."[224] Fortunately, the (politically liberal) state in which many of the largest producers and users of personal data are located has recently taken measures to stop prosecutors bent on squelching reproductive choice from obtaining records from entities in its jurisdiction. In the wake of the *Dobbs* decision, California created an exception to this out-of-state warrant compliance rule for antiabortion investigations.[225] Now, communication service providers in California are *prohibited* from complying with an out-of-state warrant if they know or should know that the warrant relates to an antiabortion investigation, and may not turn over records in response to an out-of-state warrant unless the warrant is accompanied by an attestation that the evidence is not being sought for an antiabortion investigation.[226] While we think that this update to California law was a laudable policy change, other states may enact similar laws either requiring or authorizing compliance with out-of-state search warrants.[227] This means there may well be times when their data can be legally secured for the purpose of an abortion prosecution in a different state. In sum, the legal limits on the extraterritorial acquisition of evidence are even weaker than the corresponding limits on the extraterritorial reach of criminal law. They should hence be expected to impose no great friction on restrictionist efforts to leap over borders.

4. The Geographic Fragmentation of the Personal Data Economy

The dynamics of cross-border patient search, data storage, and evidence access canvassed so far arise from the distinctive nature of post-*Dobbs* conflicts over reproductive choice. The fourth factor that is likely to thwart technology firms' attempted geographic distinctions is instead intrinsic to the personal data economy: Both the internet through which much patient search is conducted, and the personal

---

[224] CAL. PENAL CODE § 1524.2(c) (West 2022). For other examples, see State v. Rose, 330 P.3d 680, 682 (2014) (providing an example of an Oregon court issuing an out-of-state warrant, which compelled California-based Yahoo!, Inc. to provide inculpatory information from the defendant's emails); *see also* FLA. STAT. § 92.605(3) (2003) (establishing an identical requirement for Florida-based companies as the California statute).

[225] *See* A.B. 1242, 2021–2022 Reg. Sess. (Cal. 2022) (amending CAL. PENAL CODE § 1524.2(c)).

[226] CAL. PENAL CODE § 1524.2(c)(2) (West 2022).

[227] Amanda Vinicky, *Pritzker Signs Law Expanding Access to Abortion, Protecting Out-of-State Patients*, WWTV NEWS (Jan. 13, 2023), https://news.wttw.com/2023/01/13/pritzker-signs-law-expanding-access-abortion-protecting-out-state-patients [https://perma.cc/52BD-U9B4] (explaining the various legal protections that Illinois will provide to out-of-state residents seeking abortion care in the state).

data upon which prosecutors and plaintiffs rely, are not territorial in character.

The data traces created by patient search and sought by restrictionist law enforcement and civil plaintiffs will not necessarily be located in the jurisdiction in which the underlying offline activity (e.g., accessing the internet or moving through space in a way that produces locational data) previously occurred. Search for such data will focus on firms located in states that do not ban abortion. For example, some commentators have observed that in the ten states that banned abortion within a month of *Dobbs*, law enforcement had issued some 5,764 geofence warrants between 2018 and 2020, all seeking data from the California-based Google.[228] (Apple, in contrast, cannot respond to such requests because its operating system does not "store locational data in a format accessible to the company."[229]) An additional complication is that much personal data generated through commercial transactions is stored in remote cloud-computing servers.[230] These commonly use a "shard" structure whereby a "single file [is] broken into components and stored in different countries, and intelligence embedded in the network decides where to send and store the data."[231] More generally, data will "often move in ways that are disconnected with the interests of users and lawmakers."[232] The result is that requests for data made in the course of abortion regulation will increasingly be made not only to firms located outside restrictionist jurisdictions, but in respect to data located physically in yet another jurisdiction—perhaps one outside the United States. In this context, the search for information on abortion provision will inevitably cross

---

228 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 [https://perma.cc/ACW8-8W7C].

229 *Id.*

230 Riley v. California, 573 U.S. 373, 397 (2014) ("Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself."). For additional information on the growth of cloud computing, particularly during the COVID-19 pandemic, see generally Cloud Storage Market Size, Share & COVID-19 Impact Analysis, FORTUNE BUS. INSIGHTS, https://www.fortunebusinessinsights.com/cloud-storage-market-102773 [https://perma.cc/8T4H-UV8J].

231 Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1695 (2018); *accord* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 366 (2015) ("[W]hen data is stored in the cloud, it does not reside in a single fixed, observable location akin to a safe-deposit box. It may be moved around for technical processing or server maintenance reasons.").

232 Zachary D. Clopton, *Territoriality, Technology, and National Security*, 83 U. CHI. L. REV. 45, 46 (2016).

state lines in ways that implicate the sovereign and commercial interests of other states, and perhaps those of other nations too.[233]

States might also try to regulate web-based services directly in ways that have unanticipated cross-border effects. It is possible to imagine, for example, a state prohibiting non-domiciled ISPs from advertising medication abortion or offering access to URLs that give advice or provide medication abortion within that state.[234] Such efforts would at minimum create difficult legal questions related to jurisdictional conflicts and at worst imperil the sound operation of the internet. Almost since the internet's inception, there has been a vigorous debate about the feasibility and desirability of national regulation of online activity.[235] One leading contemporary account of the state of that debate characterizes the contemporary internet as "unifragged": It is a "network of networks . . . known as Autonomous Systems" that communicate to one another using a common set of data formatting and routing protocols called the "Internet Protocols."[236] This distinctive combination of dislocation and connection offers opportunities for some nationalized and state-by-state regulation.

Most fragmentation to date occurs on the national level, as governments insist on certain technical standards or prohibit foreign companies from the provision of hardware and services.[237] Only a handful of states have tried to follow suit. In 2018, California enacted a Consumer Privacy Act (CCPA). This created a range of obligations on firms that collect and use residents' personal data.[238] Some provisions explicitly target the design and form of websites. A CCPA provision that went into effect in January 2023, for example, imposes specific requirements on websites to avoid designs and practices with "the substantial effect of subverting or impairing a consumer's choice to

---

233 For a discussion of transnational cross-border discovery issues in criminal cases, and especially regarding criminal defense interests, see generally Rebecca Wexler, *The Global CLOUD, the Criminally Accused, and Executive Versus Judicial Compulsory Process Powers*, 101 TEX. L. REV. (forthcoming 2023).

234 *See supra* text accompanying notes 195–98 (discussing Aid Access and other similar websites).

235 *Compare* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) (rejecting the legitimacy of local regulation), *with* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 149 (2006) (describing the "global network . . . becoming a collection of nation-state networks").

236 MILTON MUELLER, WILL THE INTERNET FRAGMENT? 22 (2017).

237 *See* Lemley, *supra* note 90, at 1408–18 (documenting these trends).

238 CAL. CIV. CODE §§ 1798.100 to 1798.199 (West 2022).

opt-out" of selling personal information.[239] Virginia and Colorado have followed California's example in enacting statutory schemes for the protection of personal data online.[240]

These enactments demonstrate the possibility of state-specific regulation of digital communications. They are enabled in part by the fact that certain features of the unifragged internet are tightly correlated to geographic location. An IP address, for example, ordinarily conveys locational data, although it is possible (if difficult) to deploy a proxy to mask geographic inferences.[241] At the same time, parochial regulation of technical standards creates costs for local firms, which risks undermining their comparative advantage in national and global markets.[242] Moreover, it is plausible to imagine a plurality of state regulation of internet activity imposing conflicting or incompatible commands on firms. State laws such as the CCPA apply only to businesses operating in California.[243] Those firms, of course, also operate in many or all other states. The websites they host are also available across the country. The risk that other states would impose inconsistent or contrary legal obligations—e.g., must carry and must-not carry obligations in respect to telemedicine sites offering mifepristone—is clear. National intervention by Congress or the Supreme Court might resolve such conflicts. But, of course, the outcome of any constitutional challenge is hardly certain ex ante.[244]

---

239 CAL. CODE REGS. tit. 11, § 7026 (2022). The balance of the CCPA went into effect in July 2020. *See* Sanford P. Shatz & Paul J. Lysobey, *Update on the California Consumer Privacy Act and Other States' Actions*, 77 BUS. LAW. 539, 540–41 (2022) (reporting on the status of the implementation of California's consumer privacy law, and its 2021 amendment).

240 *See* VA. CODE ANN. §§ 59.1-575 to 59.1-585 (2022) (effective Jan 1, 2023) (requiring, inter alia, companies to conduct data protection assessments, enabling consumers to request companies delete their personal information, and granting consumers a right to access their data); COLO. REV. STAT. §§ 6-1-1301 to 6-1-1313 (2022) (effective July 1, 2023) (requiring, inter alia, businesses to provide consumers with clear privacy notices and conduct data protection assessments, and granting consumers the right to opt out of processing of personal data for targeted advertising, or the sale of personal data for this purpose).

241 *See* Ping Zhang, Mimoza Durresi & Arjan Durresi, *Internet Network Location Privacy Protection with Multi-Access Edge Computing*, 103 COMPUTING 473, 474–77 (2021) (discussing geolocation tools and countertools).

242 MUELLER, *supra* note 236, at 88.

243 *See* CAL. CIV. CODE § 1798.140(c)(1).

244 This possibility of conflict raises a question under Dormant Commerce Clause doctrine. *Cf.* Edgar v. MITE Corp., 457 U.S. 624, 642 (1982) (expressing concern that "if [one state] may impose such regulations, so may other States; and interstate commerce . . . would be thoroughly stifled"). We take no view here on whether a Dormant Commerce Clause challenge to state privacy regulation would prevail, and there is some reason to believe it would not. *Cf.* South Dakota v. Wayfair Inc., 138 S. Ct. 2080, 2092 (2018) ("'It has long been settled' that the sale of goods or services 'has a sufficient nexus to the State in which the sale is consummated to be treated as a local transaction taxable by that

Ultimately, we are skeptical that states could (as a practical matter) force digital platforms and other firms that employ the internet to tailor their websites to the particulars of local law, especially when this comes into conflict with other jurisdictions' commands. We think that the resulting demand to tailor websites to different states would generate fierce pressure from big tech for preemptive federal legislation, or a successful constitutional challenge. At the same time, much of the underlying technical architecture of the internet is geographically distributed across both state and national lines: Any local effort to regulate the basic technical specifications of internet traffic would create profound operational challenges and stiff public resistance.[245]

* * *

Given the flow of patients and enforcement efforts across borders, there is no clear geographic bound to the likely reach of restrictionist laws. Regulation at the confluence of abortion and the personal data economy will not, and cannot, be cabined by state borders. It will spill chaotically across the country. Even setting aside the stated ambition of some abortion opponents to prevent abortion from occurring anywhere in the nation,[246] investigative and enforcement efforts have and will keep spilling over borders.[247] Under these conditions, even compliance with presently lawful disclosure obligations places firms in the position of potentially abridging the interest in reproductive care of those who reside in states where abortion is lawful. These digital firms therefore cannot be neutral by hewing to geographic lines: Either they choose to facilitate abortion restriction in and beyond states with abortion bans—hence eliminating access to lawful reproductive care in non-restrictionist states—or they side in favor of privacy and raise the cost of restriction prosecutions.

State.'") (emphasis added) (quoting Okla. Tax Comm'n v. Jefferson Lines, Inc., 514 U.S. 175, 184 (1995)). For further analysis, see Jack Goldsmith & Eugene Volokh, *State Regulation of Online Behavior: The Dormant Commerce Clause and Geolocation*, 101 TEX. L. REV. (forthcoming 2023).

245 Another potential constraint on states' efforts is that since 2014, the Internet Corporation for Assigned Names and Numbers (ICANN) has been "accountable to the domain name community," and not the United States. MUELLER, *supra* note 236, at 102–03. ICANN's control of the domain name system also gives it a measure of control, which may limit state regulation. *See id.*

246 *See, e.g.*, Matt Berg, *Pence: 'We Must Not Rest' Until Abortion Is Outlawed in Every State*, POLITICO (June 24, 2022, 2:18 PM), https://www.politico.com/news/2022/06/24/pence-we-must-not-rest-until-abortion-is-outlawed-in-every-state-00042315 [https://perma.cc/8CAR-2P8F] (discussing Republican efforts to ban abortion in all states).

247 *See supra* text accompanying notes 185–215 for examples.

The pervasive movement of bodies, medical procedures, and data makes neutrality in the abortion wars elusive for big tech. Just as they cannot honor their obligations to employees without protecting those workers as users, firms cannot comply with restrictionist demands for information without imperiling reproductive care in states where such care is lawful. After *Dobbs*, there is simply no position of principled neutrality.

C. The Ethics of Compliance with Abortion Regulation in a Digital World

The need for tech companies to make fraught choices between reproductive care (or its absence) for both their employees and their users arises from the infeasibility of neutrality. It also arises, as we shall stress in Part III, from the pervasive need to make structural, architectural choices that either embed or dissolve privacy. These considerations mean that it is necessary to ask what does, and what should, motivate the firms that make pivotal decisions in respect to reproductive choice. To that end, we turn in this Section to the economic incentives and normative claims that might plausibly shape technology firm responses. Our aim is first to map out, as a descriptive matter, the complex motivational context in which firms make these decisions. Second, we offer a normative argument for why firms should place a thumb on the scales in favor of enlarging reproductive choice.

1. The Obligation to Maximize Shareholder Value and Profits

At the threshold, it would seem that there is a quite straightforward answer to the question of what publicly traded firms that deal in personal data—such as Meta and Alphabet—should do. A preeminent theorem in corporate law is that "corporate law should principally strive to increase long-term shareholder value."[248] A more recent alternative, associated with an August 2019 statement by the Business Roundtable, proposes that firms should strive "to deliver value to all of [a business's stakeholders]."[249] The stakeholder theory

[248] Henry Hansmann & Reinier Kraakman, *The End of History for Corporate Law*, 89 GEO. L.J. 439, 439 (2001); *see also* Leo E. Strine, Jr. & Nicholas Walter, *Conservative Collision Course?: The Tension Between Conservative Corporate Law Theory and* Citizens United, 100 CORNELL L. REV. 335, 346 (2015) ("It is hardly adventurous to assert that the predominant conservative theory of the for-profit corporation is one that embraces the view that the managers of for-profit corporations must govern the corporation with only one end in mind: the best interests of their stockholders.").

[249] *Our Commitment*, BUS. ROUNDTABLE (Aug. 19, 2019), https://opportunity.businessroundtable.org/ourcommitment [https://perma.cc/AS9M-XQXM].

is controversial, and so we focus at first on the narrower, more pecuniary shareholder-centered account.[250]

A simplistic account of shareholder-value maximization would focus on the idea that the profit margin of many firms in the digital economy is directly linked to their ability to encourage users to generate personal data that can then be monetized via behavioral advertising.[251] In 2018 alone, Facebook made $55.8 billion in revenue, mostly from behavioral advertising.[252] The approximately 307 million internet users in the United States[253] hence represent an asset whose attention, and whose digital traces, are simply to be maximized. In the reproductive-choice domain, this would entail designing platforms and apps to increase the disclosure of personal information, including about the fact and trajectory of a pregnancy. Indeed, consistent with this theory, many pregnancy tracking apps are already "based on a cultural politics that promoted self-tracking practices in order to make profit out of user data."[254] That is, they elicit disclosures through interfaces and stimuli that encourage users to engage in communications and actions that can be transformed into valuable personal data.

But even given the narrow focus on shareholder-value maximization, it is not at all clear that firms should concentrate on collecting personal data without regard for other concerns. Particularly in respect to data related to pregnancy and reproductive choice, the firms at the core of the personal data economy have a number of powerful reasons for curbing data collection. So, as a purely positive matter, the economic incentives associated with the corporate firm can end up being consistent with carefully defined cooperation with restrictionist searches, digital architectures that favor privacy ex ante, and potentially even resistance to legal process demands for abortion-relevant data.[255]

As a threshold matter, it is not the case that big tech firms maximize profits simply by hoovering up personal data. Many of those firms attract users by making strong commitments to privacy. Both

---

[250] *See, e.g.*, Lucian A. Bebchuk & Roberto Tallarita, *The Illusory Promise of Stakeholder Governance*, 106 CORNELL L. REV. 91, 94 (2020) (describing the potentially detrimental effects of a stakeholder theory of corporate governance).

[251] *See* ZUBOFF, *supra* note 51, at 80–81 (explaining how Google makes money from the behavioral data it collects).

[252] *Facebook Reports Fourth Quarter and Full Year 2018 Results*, META (Jan. 30, 2019), https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx [https://perma.cc/EE2V-7B6U].

[253] *Internet Usage in the United States–Statistics & Facts*, STATISTA (Oct. 18, 2022), https://www.statista.com/topics/2237/internet-usage-in-the-united-states [https://perma.cc/ABD9-SXHM].

[254] Barassi, *supra* note 173, at 5.

[255] For a discussion of the practicalities of each of these actions, see *infra* Part III.

Meta and Microsoft, for example, exhaustively document their own commitment to privacy in their terms of service.[256] Apple describes privacy as a "human right."[257] Its recent operating system update promotes privacy even at the cost of hindering apps' operation.[258] These verbal commitments are not new. In June 1999, Google pledged that it would be "sensitive to the privacy concerns of its users."[259] And their commitments are not limited to terms of service, but repeated even in the halls of the U.S. Capitol.[260] By deciding to repeatedly and emphatically market their services with privacy language, the management of Alphabet, Meta, Microsoft, and others express a belief that uptake of their services—and hence profits—are increased through at least some form of a verbal commitment to user privacy, and in some cases behavior that advances consumer privacy.

The belief that privacy can be a valued consumer good appears to be widely shared, with many tech firms citing customer retention and employee efficacy gains.[261] To be sure, these verbal commitments were made prior to *Dobbs* and did not directly concern reproductive choice. Moreover, they might be seen as merely cheap talk. But it

---

256 *See* Michel Protti, *Here's What You Need to Know About Our Updated Privacy Policy and Terms of Service*, META (May 26, 2022), https://about.fb.com/news/2022/05/metas-updated-privacy-policy [https://perma.cc/RDJ2-TMZ3] (explaining Meta's new privacy policy with a focus on user privacy awareness); *Microsoft Privacy Report*, MICROSOFT (Oct. 2022), https://privacy.microsoft.com/en-US/privacy-report [https://perma.cc/9YR5-H72K] (explaining Microsoft's privacy commitments and tools for maximizing user privacy); *see also* Mitchell Noordyke, *Big Tech's Shift to Privacy*, IAPP (Oct. 2019), https://iapp.org/resources/article/big-techs-shift-to-privacy-2 [https://perma.cc/2AB8-FKVW] (comparing the privacy policies of major technology corporations).

257 *Privacy*, APPLE, https://www.apple.com/privacy [https://perma.cc/Y8UB-ZNUD].

258 *See* Laurel Wamsley, *Apple Rolls Out Major New Privacy Protections for iPhones and iPads*, NPR (Apr. 26, 2021, 4:12 PM), https://www.npr.org/2021/04/26/990943261/apple-rolls-out-major-new-privacy-protections-for-iphones-and-ipads [https://perma.cc/2NUE-FC9W] (describing Apple's push for data privacy protections for its users and noting the potential cost to Facebook and other app-based offerings).

259 Charlie Warzel & Stuart A. Thompson, *Tech Companies Say They Care*, N.Y. TIMES (Apr. 10, 2019), https://www.nytimes.com/interactive/2019/04/10/opinion/tech-companies-privacy.html [https://perma.cc/49D9-WRXG] (analyzing tech companies' privacy policies for language about protecting users).

260 *See* David Shepardson, *House Republicans Query Apple, Alphabet on Privacy, Data Practices*, REUTERS (July 9, 2018, 3:41 PM), https://www.reuters.com/article/us-congress-privacy-tech/house-republicans-query-apple-alphabet-on-privacy-data-practices-idUSKBN1JZ2KG [https://perma.cc/75EX-GR8L] (citing public statements from Alphabet in response to congressional inquiries that highlight the company's commitment to user privacy).

261 *See, e.g.*, Melanie English, *How Businesses Benefit From Investing in Privacy*, TERAMIND (Apr. 9, 2021), https://www.teramind.co/blog/investing-in-privacy [https://perma.cc/57LP-RETT] ("Privacy invested companies of all sizes reported noticeable returns across all areas of their business. Greater customer growth and retention, a one up on competitors and increased productivity can all be achieved by putting privacy front and center.").

would be startling if a legal change that made privacy-respecting reproductive choice more valuable to users led companies to treat such privacy with less solicitude.

Given the demographics of the personal data market, solicitude of privacy-enabling reproductive choice is likely a sound exercise of business judgment by such platforms when one considers their expected customer base. Over time, the trend has been for women to become more frequent users of social media than men.[262] Women are (slightly) more likely to support legal abortion than men.[263] Further, unsurprisingly, younger tranches of the population are also more likely to use social media than older ones.[264] On Facebook, the most-represented age cohort is between twenty-five and thirty-four years old.[265] The age cohorts that engage most frequently also evince the strongest support for access to abortion care. For example, people between the ages of eighteen and twenty-nine years show the highest support for legalizing abortion in all or most cases.[266] It would seem at best negligent—and at worst an abuse of discretion—for these firms to adopt an approach to privacy that alienated and angered their present and future core constituencies.[267] Solicitude for privacy around

---

[262] *Social Media Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media/?menuItem=45b45364-d5e4-4f53-bf01-b77106560d4c#panel-45b45364-d5e4-4f53-bf01-b77106560d4c [https://perma.cc/MXB9-BHPC].

[263] *Public Opinion on Abortion*, PEW RSCH. CTR. (May 17, 2022), https://www.pewresearch.org/religion/fact-sheet/public-opinion-on-abortion/#h-views-on-abortion-by-gender-2022 [https://perma.cc/86QA-D8GC].

[264] *Social Media Fact Sheet*, *supra* note 262.

[265] Brent Barnhart, *Social Media Demographics to Inform Your Brand's Strategy in 2022*, SPROUT SOCIAL: SPROUT BLOG (Mar. 2, 2022), https://sproutsocial.com/insights/new-social-media-demographics [https://perma.cc/CCY9-FJNR]. Unsurprisingly, younger users flock to networks such as Instagram rather than LinkedIn or Facebook. *See* Alyssa Hirose, *114 Social Media Demographics that Matter to Marketers in 2022*, HOOTSUITE (Apr. 5, 2022), https://blog.hootsuite.com/social-media-demographics/#Instagram_demographics [https://perma.cc/696U-PMJ9] (noting that Instagram is the most-used social media platform among American teenagers).

[266] *Public Opinion on Abortion*, *supra* note 263; *'Pro-Choice' or 'Pro-Life' Demographic Table*, GALLUP, https://news.gallup.com/poll/244709/pro-choice-pro-life-2018-demographic-tables.aspx [https://perma.cc/C5SP-XU8B]; *see also* Daniel Cox, *There's a New Age Gap on Abortion Rights*, FIVETHIRTYEIGHT (June 1, 2022, 6:00 AM), https://fivethirtyeight.com/features/theres-a-new-age-gap-on-abortion-rights [https://perma.cc/3WE6-TFCA] (underscoring the relative historic novelty of an age gap on attitudes towards abortion between generations).

[267] For select examples of scholarly work from an in-depth and ongoing academic debate concerning whether loyalty to users' data privacy interests is or is not compatible with firms' fiduciary duties to their shareholders, see Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356 (2022) (proposing a model for legislating data loyalty based on loyalty's well-established principles in other parts of the law); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021) (advocating for the creation of a duty of loyalty for

reproductive care, therefore, is arguably consistent with and may even advance the pecuniary goals of many publicly traded firms in the personal data economy.

Even with respect to governmental demands for data, Alan Rozenshtein has argued that big tech also has financial incentives to limit ex ante their exposure to such demands, and to insist on rigorous compliance with the law before data is released. Doing so, he contends, lowers the transaction costs of ordinary business and "can also improve a company's global competitiveness."[268] He also invokes "ideological" reasons for favoring privacy linked to a worldview among management and engineers that is "libertarian in politics."[269] Rozenshtein might have added that firms in this sector of the economy might commit to privacy because doing so allows them to attract and retract higher quality workers, who would otherwise have other options for employment.[270] As Rozenshtein shows, these incentives might lead companies to be sticklers for procedural compliance, and otherwise opt for pro-privacy structural defaults that raise search costs for government actors in general. We think that his logic applies a fortiori in respect to reproductive privacy given that desirable workers are likely to be young, and hence more inclined to support broader access to reproductive choice.

We recognize that not all relevant incentives cut in the same direction. Data brokers, in particular, have not made public privacy commitments and have not abated their trade in pregnancy-related information since *Dobbs* because their financial incentives cut in favor of accelerating, not slowing down, that trade.[271] We would not anticipate that data brokers will change their behavior absent legal intervention. Their business model does not depend on customer retention or on hiring the brightest minds for data analytics. Instead, their profits come from arbitrage. So they are more likely to be indifferent

---

personal information that would bind data collectors to act in the best interest of the people exposing their data online); Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019) (critiquing the information-fiduciary model as both inadequate to the scale of the challenge it seeks to solve and encouraging complacency in platform regulation); Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020) (summarizing the information-fiduciary model and defending it against Khan and Pozen's critique).

268 Rozenshtein, *supra* note 67, at 116–18.

269 *Id.* at 118.

270 *Cf.* Daniel Hemel & Dorothy S. Lund, *Sexual Harassment and Corporate Law*, 118 COLUM. L. REV. 1583, 1655–56 (2018) (making this same point about sexual harassment in corporate organizations).

271 *See* Ng, *supra* note 130 (discussing data brokers' unwillingness to stop offering information on pregnant people due to business incentives).

to the moral objections to sharing data so as to enable the coercive regulation of abortion.

We would further expect to see conflict even within companies and boards. Abortion is a profoundly divisive moral question on which individual equity holders sharply disagree. Corporate management could reasonably conclude that it has strong reasons simply to avoid controversy and to steer clear of positions that divide equity holders. But this position overstates the legal interest of shareholders.[272] To see this, consider the extent to which shareholders can influence corporate political actions. Under existing corporate law, decisions about controversial political speech are made exclusively by management with no input from shareholders or independent directors and without any mandatory disclosure to investors.[273] In consequence, equity holders have no say on whether a firm makes donations to Republicans or Democrats, or even (say) avoids donations to candidates who supported the violent January 6, 2021 insurrection. If shareholders have no cognizable legal interest in what political positions and expenditures a firm makes, it is hard to see why they would have a legal interest in matters of digital privacy that bite hard on customers' and employees' interests. Nevertheless, it seems plausible to think that there is some risk that a public controversy over a company's stance on abortion could detract from the brand or from a firm's capability to generate profits in the long term, raising concerns from a shareholder-maximization perspective.

The problem, then, boils down to a practical one. Even if firms strive to sit on the sidelines, as we have stressed above, there is no neutral position in the post-*Dobbs* abortion battlefield: There is no way, that is, of remaining above the fray. If the taking of any position risks backlash, then the more important question is which position is ultimately warranted.

---

272 *But see* Oliver Hart & Luigi Zingales, *Companies Should Maximize Shareholder Welfare Not Market Value* 28 (Eur. Corp. Governance Inst., Finance Working Paper No. 521/2017, 2017), https://ssrn.com/abstract=3004794 [https://perma.cc/A6WL-9L22] (arguing in favor of allowing shareholders to vote on corporate policy on the ground that their welfare is not equivalent to mere maximization of share price). Hart and Zingales would limit their approach to cases in which equity holders have "prosocial" views; of course, what that means in the abortion-related context is sharply contested. *Id.*

273 *See* Lucian A. Bebchuk & Robert J. Jackson, Jr., *Corporate Political Speech: Who Decides?*, 124 HARV. L. REV. 83, 87 (2010) (describing the limited role shareholders play in corporate speech decisions); *see also* Elizabeth Pollman, *Citizens Not United: The Lack of Stockholder Voluntariness in Corporate Political Speech*, 119 YALE L.J. ONLINE 53, 53 (2009) ("[W]hen corporations are allowed to spend general funds on electoral advocacy, stockholders may have money they invested in a corporation used for political advocacy they oppose.").

2. *Why Firms Should Favor Privacy as a Matter of Principle*

We now turn from the positive to the normative: Are there compelling arguments that sound in public values for big tech firms to favor privacy around reproductive choice? And—more controversially—would it be legitimate for companies not just to build in privacy by default and insist on strict procedural compliance by the government, but also to actively push back on restrictionist demands for information using all the tools that law makes available? Further, what of outright defiance, which might be called "corporate civil disobedience"? The question proves, surprisingly, more complex than it might at first blush seem.

To begin with, it is plausible to think that digital platforms in particular are under a social (if not a legal) obligation to promote truthful rather than empirically false speech. Platforms are routinely criticized for "pollution of the democratic environment through fake news, junk science, computational propaganda and aggressive micro-targeting and political advertising."[274] A premise of these criticisms is that it is appropriate for society (if not the state) to demand that these firms avoid what might be called "negative epistemic externalities." Much as we make the moral demand that manufacturers avoid the emission of noxious gases that impose costs on human health or the environment, even when such forbearance is not compelled by law, so too we can make demands of big tech. This kind of a moral demand for truthfulness has a direct application in the context of abortion-related speech and activity online. The epistemic quality of patient search is a function of platforms' willingness to ensure the priority of truthful over misleading speech and to preserve access to websites and voices that offer truthful information about the medical implications of reproductive choice. If platforms are properly criticized for failing to eliminate COVID-19 misinformation,[275] then they are also subject to moral condemnation when they do not provide direct and unfiltered access to medically accurate information on reproductive choice.[276]

---

[274] Helen Margetts, *Rethinking Democracy with Social Media*, 90 POL. Q. 1, 1 (2019); *see also* Nathaniel Persily & Joshua A. Tucker, *Introduction*, *in* SOCIAL MEDIA AND DEMOCRACY: THE STATE OF THE FIELD, PROSPECTS FOR REFORM 1, 2 (Nathaniel Persily & Joshua A. Tucker, eds. 2020) (offering a similar list that includes "disinformation, polarization, echo chambers, hate speech, bots, political advertising, and new media"); Ronald J. Deibert, *The Road to Digital Unfreedom: Three Painful Truths About Social Media*, 30 J. DEMOCRACY 25, 31 (2019) (asserting that social media "may be one of the main reasons why authoritarian practices are now spreading worldwide").

[275] *See* Dawn Carla Nunziato, *Misinformation Mayhem: Social Media Platforms' Efforts to Combat Medical and Political Misinformation*, 19 FIRST AMEND. L. REV. 32, 37–51 (2020) (discussing efforts by platforms to address pandemic-related misinformation).

[276] We bracket here firms' pecuniary incentive to ensure accuracy in search.

What, though, of the claim that firms have an obligation to maximally comply with the law, and as such must extend as much cooperation to restrictionist prosecutors and civil plaintiffs as is technologically feasible? We think that such a broad claim is untenable. A starting point for thinking about this idea is that the choices made by firms in the personal data economy have effects on the availability of reproductive care not only in restrictionist states, but also in states where abortion is available and protected by law. Firms hence are not confronted by just one set of legal claims: There is law pushing in both directions. Firms necessarily have degrees of freedom in balancing different jurisdictions' competing and inconsistent legal demands.

There is nothing particularly new in this. The global nature of the internet means that platforms and search firms have long been faced with tricky choices about how to manage access and data flows in the teeth of divergent national legal regimes.[277] *Dobbs* just recreates that international dynamic within the bounds of the nation-state.

The choices confronting firms, moreover, are not whether to directly provide reproductive care, but whether to create an informational environment characterized by privacy for patients or not.[278] The value of such privacy weighs against the abstract value of legal compliance. Some forty years ago, Frank Easterbrook and Daniel Fischel pointed out that "[m]anagers have no general obligation to avoid violating regulatory laws, when violations are profitable to the firm . . . . We put to one side laws concerning violence or other acts thought to be *malum in se*."[279] Their perspective, predictably, elicited objections.[280] Yet more recently, scholars have pointed to the large social gains from corporate willingness to push on the edges of the law, as

---

[277] *See, e.g.*, evelyn douek & Genevieve Lakier, *First Amendment Politics Gets Weird: Public and Private Platform Reform and the Breakdown of the Laissez-Faire Free Speech Consensus*, 2022 U. CHI. L. REV. ONLINE *1, *11 (2022) (discussing "fears of a 'race to the bottom' for free expression in which the most restrictive jurisdiction determines the rules that govern speech online everywhere").

[278] There is an argument that some personal data ranks as speech protected by the First Amendment. *See* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 61 (2014) ("If the dissemination of mechanical recordings receives First Amendment protection (which it does), then the creation of those same recordings must have First Amendment significance, too." (footnote omitted)).

[279] Frank H. Easterbrook & Daniel R. Fischel, *Antitrust Suits by Targets of Tender Offers*, 80 MICH. L. REV. 1155, 1168 n.36 (1982) (citations omitted).

[280] *See, e.g.*, Leo E. Strine, Jr., Lawrence A. Hamermesh, R. Franklin Balotti & Jeffrey M. Gorris, *Loyalty's Core Demand: The Defining Role of Good Faith in Corporation Law*, 98 GEO. L.J. 629, 653 n.71 (2010) ("American corporate law embeds law compliance within the very mission of the corporation. Loyalty to the corporation's obligation as a citizen to attempt in good faith to abide by the law is not incidental to a director's duties, it is fundamental.").

well as the frequency with which it happens. For example, Elizabeth Pollman has identified numerous complexities in corporate compliance with the law, noting that while "a great deal of this activity is socially harmful, some corporate disobedience has the potential to produce value or catalyze legal change."[281] Relevant here, she identifies a long history of "companies that violate or refuse to comply with laws that are moralistic in nature."[282] More recently, religious corporations have been prominent challengers of regulations they view as morally unacceptable.[283] Of course, those firms made claims for religious exemptions related to their religious beliefs. But digital privacy in respect to reproductive privacy turns on moral claims that, in our view, are equally normatively compelling on behalf of those who wish to access accurate information and secure life- and health-preserving medical care.[284] Often they are claims with a profound religious or philosophical pedigree. It is the rankest prejudice to assume that a firm's objection to contraception for its employees deserves moral weight, while denying the same with respect to a firm's objection to assisting the suppression of reproductive choice.

* * *

There is, therefore, no neutral option for big tech firms in the coming abortion wars. They cannot claim to protect employees while leaving them exposed as users. Nor are there tractable geographic lines that can be demarcated. Even aside from the fact that firms must set structural defaults that determine whether user privacy is even feasible (or to what extent it can ever be realized) in the first instance, their economic incentives and interest in a reputation for truthfulness push in favor of facilitating reproductive care. The counterargument that they must strictly comply with law not only ignores the fact of

---

281 Elizabeth Pollman, *Corporate Disobedience*, 68 DUKE L.J. 709, 718 (2019).

282 *Id.* at 742.

283 *See, e.g.*, Burwell v. Hobby Lobby Stores, Inc., 573 U.S. 682, 688–91 (2014) (upholding a corporation's challenge to a government mandate to provide health insurance for contraception under the Religious Freedom Restoration Act).

284 *Cf.* BRIAN LEITER, WHY TOLERATE RELIGION? 63 (2013) ("[T]here is no apparent moral reason why states should carve out special protections that encourage individuals to structure their lives around categorical demands that are insulated from the standards of evidence and reasoning we everywhere else expect to constitute constraints on judgment and action . . . ."). Prohibitions on abortion also implicate the religious freedoms of groups who believe in the "necessity" of such care. *See* Brendan Pierson, *Florida Abortion Ban Violates Jews' Religious Freedom, Lawsuit Says*, REUTERS (June 14, 2022, 6:07 PM), https://www.reuters.com/world/us/florida-abortion-ban-violates-jews-religious-freedom-lawsuit-says-2022-06-14 [https://perma.cc/P5RF-A4CZ] (discussing a lawsuit that alleges that a Florida abortion ban violates Jewish religious freedom because Jewish law requires the procedure in some cases).

underlying legal pluralism and conflict post-*Dobbs*, but it also ignores the complex normative considerations attending different forms of corporate disobedience.

In short, both as a positive and as a normative matter, there is no good reason to assume that firms in the personal data economy cannot or should not advance the privacy interests of pregnant persons. To the contrary, it would be a plausible exercise of business judgment for them to do so.

III
The Digital Battlefields of the Coming Abortion Wars

With this orientation toward choice in mind, we turn to a taxonomy of "digital battlefields" in the coming abortion war on which the production and use of abortion-related information will be contested. We bracket here the important question whether internet search engines' algorithms, such as Google's, will be optimized to generate accurate or misleading results. The question of search-engine design is an important predicate matter, but somewhat at an angle to the questions of investigative tactics we excavate here.

This Part describes four primary battlefields, or sites for contestation, in respect to surveillance and access to the digital trail left by patients' search. These concern, respectively: (1) firms' decisions to collect and retain data; (2) firms' responses to regulators' demands for information; (3) firms' provision of privacy-protective infrastructure to enable individual users to access accurate information privately and securely; and (4) federal and state legislative action to shield abortion-relevant data from restrictionist law enforcement and civil plaintiffs.

In presenting these four sites, we assume the moral perspective that technology companies should take on primary responsibility for creating the conditions in which privacy for reproductive choice is best realized. We stress that reliance upon individual users to adopt protective measures should not be a first resort given the varied epistemic and social capital possessed by pregnant persons, and the likelihood that a strategy of self-reliance when it comes to digital privacy would leave most exposed those who are most likely to be subjected to coercive state regulation.[285] We note in advance that choices on one battlefield influence the fight in others: From a privacy perspective, for

[285] Prince makes a similar point that relying on individuals to "protect[] [their] reproductive health privacy through self-management" imposes "a Herculean, if not impossible task." Prince, *supra* note 40, at 41. *But see* Fowler & Ulrich, *supra* note 41, at 73–75 (arguing that a "crusading minority" of informed and empowered users can help to increase privacy protections for all users of period and fertility trackers).

example, eliminating data collection and retention renders resistance to law enforcement demands otiose. We conclude this Part by laying out a concrete, immediately actionable proposal that federal and state legislatures should enact statutory evidentiary privileges to make abortion-relevant data immune from compulsory legal process and inadmissible in restrictionist court proceedings.

A. Non-Collection and Non-Retention of Information

Because technology companies cannot remain neutral in the face of law enforcement and private efforts to access patient search data,[286] they should in the first instance minimize the range of hard choices that they have to make. This is desirable not least because it tamps down on internal conflict within the firm over reproductive choice and minimizes their exposure to external criticism. In practice, this would mean that firms should reduce patients' exposure to harmful disclosures in the first instance by limiting the kinds of information collected and retained, curbing their economic reliance on resale, and minimizing the possibility of inference of individual attributes relevant to pregnancy and abortion using machine-learning tools.

This is not simply a question of changing firms' privacy policies from opt-out to opt-in default collection and use. Privacy law scholars have warned for years against relying on notice and consent policies that task individual users with the burden of protecting data from tracking, storage, and resale. This is an ineffective way to realize substantive privacy protection.[287] More concretely, firms should undertake "significant corporate responsibilities in addition to a substantive system of individual rights."[288] Regardless of individual user consent, firms that fail to make affirmative commitments to non-collection and non-retention of abortion-relevant data will not be neutral: They will be choosing to facilitate restrictionist prosecutions and civil actions above and beyond anything that the law requires.

Curtailing most firms' collection and retention of abortion-relevant data is feasible both technically and economically. We have already flagged one example: In the wake of *Dobbs*, Google

---

286 *See* discussion *supra* Sections II.A–B.

287 *See, e.g.*, Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 295 (2011) ("[The] incompleteness of a reliance on formal notice and consent mechanisms alone to protect against real harms as rapid technology changes reduce the power of individuals to isolate and identify the use of data that concerns them."); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1696 (2020) (advocating "skeptic[ism] of the role of consent in validating data practices").

288 Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 96 (2020).

announced that it would start proactively deleting users' location information tracking them to abortion clinics and other sensitive health care providers.[289] That commitment matters even beyond providing individuals with a zone of plausible deniability as to their whereabouts if their phones are searched or their data subpoenaed. It will also preclude law enforcement from seeking geofence warrants. To date, law review scholarship and policy debates have argued that geofence warrants are constitutionally suspect, and at least one federal district court has held them to be unconstitutional general warrants.[290] But most courts have still permitted their use.[291] The erasure of locational data means that litigation over the specific legal or constitutional constraints on these warrants becomes irrelevant. The net effect is to eliminate an important source of uncertainty for patients without precipitating a frontal confrontation with law enforcement.

While Google's action is a promising first step, it hardly covers the waterfront of a pregnant person's exposure as a consequence of digital search. Law enforcement currently uses warrants to collect bulk information about all the IP addresses that search particular keywords on the internet.[292] Here, Google and other technology companies should also commit to non-collection and non-retention of any identifying information associated with abortion-relevant web searches. Further, they should preemptively disable their own internal, automated scanning of message and email contents for abortion-relevant text. Under this approach, information that could be targeted for restrictionist legal process would never be collected in the first place.

If companies must collect abortion-relevant data essential to the provision of their services, then there are still steps that they can and should take to mitigate privacy-related risk to users—again without

---

289 *See supra* text accompanying note 171.

290 *See* United States v. Chatrie, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022) (invalidating a geofence warrant on Fourth Amendment grounds).

291 *See Geofence Warrants*, *supra* note 99, at 2509 (noting that thousands of individuals are made suspects through the use of geofence warrants); *see also supra* text accompanying notes 98–99 (discussing such warrants).

292 *See* Conti-Cook, *supra* note 37, at 56 ("Prosecutors and investigators could potentially subpoena ISP's for the IP addresses of every search for 'abortion medication' or 'abortion pills' or any other keyword combination."). Another investigative tool is the Network Investigative Technique, or "NIT," which sends instructions to a user's computer that cause the activating computer to transmit certain information to a government computer, including the activating computer's actual IP address, that can help identify users of a particular website who otherwise would not be found. *See* Kurt C. Widenhouse, Note, *Playpen, the NIT, and Rule 41(b): Electronic "Searches" for Those Who Do Not Wish to Be Found*, 13 J. BUS. & TECH. L. 143, 144 (2017) (describing the use of a NIT in a sting operation to arrest hundreds of users of a child pornography website).

precipitating a legal conflict. To begin with, they should purge nonessential elements and engage in routine deletion and data minimization procedures at regular intervals. Users should have rights to delete data remotely. These should be relatively costless to exercise. Firms should also disable third-party tracking entirely and forego the use of predictive analytics to infer attributes of pregnancy and abortion.[293] Storing data locally on users' devices, instead of in the cloud, offers some additional protection from geofence searches, even though law enforcement can still obtain a warrant to search the devices directly. Offering end-to-end encryption by default for all communications will also help, although this solution is imperfect because metadata would remain available for compelled disclosure.

Finally, for any personal data that must be retained for commercial reasons, firms should decouple the data from personally identifying information to the greatest extent possible.[294] This may include offering users anonymous and pseudonymous accounts and adopting differential privacy protections before sharing data with outsiders.[295] Even if reidentification remains technically feasible, these actions will at least add some friction to slow the identification process and thus reduce the capacity for law-enforcement and vigilante uses.

B. Non-Cooperation with Disclosure Demands

Choosing not to collect and not to retain abortion-relevant data is the best way to protect pregnant people's access to abortion care while complying with the law. But there are also second-best options. Firms that fail to reform their collection and retention policies, or that must collect and retain a certain amount of sensitive data as essential adjuncts to their provision of services, should leverage their outsized footprints in the information and law-enforcement ecosystems to make abortion prosecutions more, rather than less, costly to pursue.

---

[293] For example, Facebook tracks users' interactions with the Facebook platform (e.g., posts, groups, friends, physical location), and through partnerships with marketers, it tracks off-Facebook activity of anyone, including nonusers, who visits a Facebook partner's site. *See* David Nield, *All the Ways Facebook Tracks You—and How to Limit It*, WIRED (Jan. 12, 2020, 7:00 AM), https://www.wired.com/story/ways-facebook-tracks-you-limit-it [https://perma.cc/F5M7-M9DZ] (describing all of the ways Facebook tracks user data).

[294] For a useful, if dated, overview of deidentification techniques, see SIMSON L. GARFINKEL, NAT'L INST. STANDARDS & TECH, U.S. DEP'T COM., NISTIR 8053, DE-IDENTIFICATION OF PERSONAL INFORMATION (2015), https://csrc.nist.gov/publications/detail/nistir/8053/final [https://perma.cc/4BRD-A93W].

[295] On the use of pseudonyms in financial contexts, see Adam Candeub, *Privacy and Common Law Names: Sand in the Gears of Identification*, 68 FLA. L. REV. 467, 499–502 (2016).

They can do so by choosing not to cooperate voluntarily with law enforcement or vigilante attempts to acquire abortion-relevant data.

Non-cooperation, to be clear, need not reach the level of civil disobedience. Nor need it subject a firm to the risk of costly legal liability.[296] On the contrary, technology companies can go a long way toward protecting pregnant people's privacy simply by reducing the alacrity and ease with which restrictionist actors can access data. Of course, the opposite is also true: If firms elect to process abortion-relevant data demands using standard procedures, they will be making the choice to aid antiabortion prosecutions. The following discussion lays out some of the options that firms have and the actions they should take to advance privacy.

To begin with, technology companies should commit to not volunteering data to law enforcement or vigilantes.[297] Most obviously, this means not initiating disclosures of abortion-relevant data and refusing to comply with law enforcement or vigilante requests unaccompanied by valid legal process. But given the secondary market for personal data, the obvious precautions of requiring a valid warrant or subpoena are not sufficient to promote patient privacy or enable patient search. If personal data reaches private intermediaries engaged in the secondary market, those intermediaries may in turn sell or give it to vigilante bounty hunters or law enforcement, entirely circumventing the protections of legal process.[298] Hence, a robust commitment not to volunteer abortion-relevant data also requires not sharing or selling the data to intermediaries that may then offer access to restrictionist law-enforcement and private actors.[299]

---

296 *See supra* Section II.C (discussing corporate disobedience).

297 *Cf.* Rozenshtein, *supra* note 67, at 125–27 (discussing such voluntary compliance).

298 *See* CAREY SHENKMAN, SHARON BRADFORD FRANKLIN, GREG NOJEIM & DHANARAJ THAKUR, LEGAL LOOPHOLES AND DATA FOR DOLLARS: HOW LAW ENFORCEMENT AND INTELLIGENCE AGENCIES ARE BUYING YOUR DATA FROM BROKERS 7 (2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf [https://perma.cc/KL7X-6UQM] (describing the mechanisms by which law enforcement acquires data from third party brokers); *see also* Fourth Amendment Is Not For Sale Act, H.R. 2738, 117th Cong. (2021) (proposing a ban on law enforcement purchasing data from brokers).

299 Indeed, European law already mandates that if a firm relies on consent as the legal basis for data processing, it is not allowed to switch the legal basis from consent to another basis even if this other valid basis (such as legitimate business interest) has always existed. *See* Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 36; Eur. Data Prot. Bd., *Guidelines 05/2020 on Consent under Regulation 2016/679*, at 25 (May 4, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [https://perma.cc/PF69-6Y7P]. Another possibility is that firms selling data condition the sale on the purchaser's

To be sure, electing not to share or sell certain data to brokers and other third parties will likely create economic costs for technology companies. Beyond the obvious loss in data sales, companies may have to undertake costly data processing and analysis in-house, rather than contracting out for cheaper services. But for companies where abortion-relevant data remains a small percentage of the overall business model, such as Alphabet or Meta, these costs should be relatively limited—and potentially offset in terms of gains among users who value privacy related to reproductive choice.[300] And for companies where abortion-relevant data is a substantial part of the business model, such as period-tracking, or other reproductive health apps that may specialize in predicting pregnancies or identifying new parents for advertisers, limiting unnecessary risk to their users should be viewed as a necessary cost of doing business without compromising important privacy interests—much as pollution control may be an appropriate cost incurred by manufacturers. There are plenty of data sources from which to profit. Seeking pecuniary gain by trafficking in data that puts users' intimate privacy at risk without installing appropriate safeguards should not be one of them.

Technology companies should also commit to raising legal process transaction costs. Many major technology companies have a two-tier system for responding to legal process demands for user data. One tier is an efficiency-maximizing online system available solely to law enforcement requesters.[301] The other tier, available to nongovernmental litigants including criminal defendants, requires slower and more onerous service of process.[302] This system reduces the transaction costs for law enforcement, and comparatively increases those costs for nongovernmental litigants. This lever is well-established, fully lawful, and entirely within the power of technology companies to manipulate at will. Here is how it currently works.

Firms play a substantial role in modern law enforcement. Major technology companies receive thousands of law enforcement requests for user data every single day. For instance, Google reported that law enforcement entities within the United States made 50,907 requests for information from 115,594 unique accounts during just the period

compliance with certain terms. The feasibility of this approach, however, turns on the frequency with which data is sold. If there is rapid turnover in data trading, with many counterparties exchanging data at speed and at volume, the imposition of specific use conditions may be difficult to achieve or enforce.

300 *Cf. supra* text accompanying note 261 (suggesting reasons privacy can be a profitable tactic for a data firm).

301 *See infra* text accompanying notes 306–08.

302 *See infra* text accompanying notes 309–11.

from January to June 2021.[303] During the same period, Meta reported 63,657 requests for information from 111,117 accounts[304] and Twitter reported 3,000 requests for information from 7,133 accounts.[305] Processing and responding to that volume of requests takes time and personnel. To accelerate the process and to create economies of scale, many companies have built special online "portals" that maximize efficiency and waive requirements for in-person service of process.[306] Law enforcement requesters certify their identity via these portals and upload digital copies of their warrants or subpoenas.[307] The requests then go directly to human reviewers inside the companies, who sometimes reach out to a law enforcement requester for clarifying information before providing responsive data in an easily downloadable format.[308] This portal system reduces transaction costs for companies and law enforcement alike.

But not all legal process requests receive this special treatment. Many companies do not currently permit nongovernmental litigants to use the online portals, so these litigants must follow the standard service of process rules for their subpoenas. For instance, when criminal defense counsel seek data from technology companies, their requests are shunted to a second-tier process seemingly designed to maximize inefficiency.[309] Not only are defense counsel barred from using the online portals, but also some major technology companies will not even accept in-person service of process on their company representatives located in the counsel's state. For instance, criminal defense counsel in New York who wish to subpoena Facebook or Meta may

---

303 *Google Transparency Report: Global Requests for User Information*, GOOGLE, https://transparencyreport.google.com/user-data/overview?hl=EN&user_requests_report_period=series:requests,accounts;authority:US;time:&lu=legal_process_breakdown&legal_process_breakdown=expanded:0 [https://perma.cc/8GNY-V3MS].

304 *Meta Transparency Center: United States*, FACEBOOK, https://transparency.fb.com/data/government-data-requests/country/US [https://perma.cc/SGH7-4YET].

305 *Twitter Transparency: United States*, TWITTER, https://transparency.twitter.com/en/reports/countries/us.html#2021-jan-jun [https://perma.cc/FE2S-CHMJ].

306 *See, e.g.*, *Law Enforcement Online Requests*, FACEBOOK, https://www.facebook.com/records/login [https://perma.cc/D8GB-7ZY6]; *Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines [https://perma.cc/E4FK-CR2Y] ("Law enforcement officials who do not submit requests through the Law Enforcement Online Request System should expect longer response times.").

307 *Law Enforcement Online Requests*, *supra* note 306.

308 *See* Yan Fang, *The Managerialization of Search Law and Procedure for Internet Evidence* 12–19 (Working Paper, 2022) (on file with author) (articulating law enforcement compliance procedure within companies).

309 *See, e.g.*, *Can I Obtain Information About Someone's Instagram Account?*, INSTAGRAM, https://help.instagram.com/232762833582105 [https://perma.cc/PJH4-QQEL] (requiring that if a private entity wishes to serve a subpoena on Meta Platforms, Inc., "the subpoena must be a valid federal, California or California domesticated subpoena").

have to domesticate their subpoena into California law through the California courts.[310] For indigent public defenders without a national network of attorney-partners willing to bring out-of-state subpoenas to the California courts for enforcement, and without excess funds to hire out-of-state process servers, this requirement alone can effectively preclude all access to Meta data.[311]

Whatever the costs of this arrangement for fairness in criminal adjudication, this two-tier filtering structure is an opportunity in the post-*Dobbs* context. Firms should modify their systems for responding to legal process to vary transaction costs depending on whether the entity demanding the data can certify that the information is not for an abortion-relevant legal suit. They could operationalize this policy easily by conditioning law enforcement's access to the hyper-efficient online portals on submission of an affidavit that the alleged crime under investigation concerns a specific list of topics that exclude abortion.[312] Absent such an affidavit, firms would treat law enforcement service of process the same way they now treat criminal defense subpoenas. If the second-tier system has been lawful and adequate for criminal defense counsel (and civil litigants) across the country, then that same second-tier system should be lawful and adequate for law enforcement requests as well.

In considering this proposal, it is important to remember that technology companies need not even implement any novel infrastructure or procedures to slow legal process for interstate collection of data by antiabortion regulators. It is enough that they allocate restrictionist warrants and subpoenas to the same processing track that they currently employ for criminal defense counsel and subpoenas in civil cases.

C. Challenging Legal Process Demands in Court

Even in extreme cases where regulators demanding data have what appears to be a valid warrant or subpoena, there may be opportunities for companies to move to quash the legal process in court. Importantly, the initial ex parte process whereby law enforcement officers seek warrants, generally from a magistrate judge, can amount

---

310 *See* Kashmir Hill, *Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone.*, N.Y. TIMES (Nov. 22, 2019), https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html [https://perma.cc/P9SG-7BYF] (stating that public defenders in New York need a California judge's approval for a subpoena of Facebook).

311 *See, e.g.*, *id.*

312 Hence, this would not impose a friction on prosecutions for noncontroversial offenses, say, involving domestic violence, stalking, cyberbullying, or child exploitation and pornography.

to little more than a rubber stamp.[313] No adverse party is present to advocate for limiting the scope of the warrant or to represent the privacy interests of the investigative target. Meanwhile, many subpoenas require even less burdensome threshold showings. Most pre-indictment subpoenas from law enforcement need not be reviewed ex ante by a judge at all.[314] Even civil subpoenas can be issued by an attorney alone, with no ex ante judicial oversight.[315] It is not until the recipient of a warrant or subpoena challenges its scope or validity in court that these forms of legal process trigger full adversarial scrutiny. To fully vindicate constitutional and statutory privacy protections, therefore, recipients of legal process must go to court and bring motions to quash.

Given this legal context, companies should not presume that even warrants and subpoenas that initially seem on their face to be valid are, in fact, lawful. Instead, tech firms should commit publicly to challenging the scope and validity of all abortion-related legal processes they receive. Successful challenges will end a disclosure demand. Meanwhile, even challenges that ultimately do not receive a favorable ruling in court will nonetheless raise the costs (and slow the pace) of restrictionist search activity in a fashion that accords with users' privacy expectations and firms' ex ante commitment to privacy.[316] Of course, any such challenges must have a non-frivolous legal basis. But there are three common, wholly non-frivolous legal challenges that technology companies should make to contest legal process demands: (1) challenges to the jurisdictional reach of the issuing court; (2) challenges to the scope and validity of the process; and (3) challenges to any accompanying non-disclosure orders that purport to bar the recipient firm from notifying the target of the investigation.

---

313 *Cf.* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313 (2012) (discussing excessive sealing of magistrate judge "warrant-type applications").

314 *See, e.g.*, Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 805 & nn.2–3 (noting that in most states prosecutors issue grand jury subpoenas directly, and that these along with administrative subpoenas are not reviewed by the courts until "they are resisted by the target").

315 *See, e.g.*, FED. R. CIV. P. 45(a)(3) (authorizing attorneys to issue and sign subpoenas).

316 Prior scholars have proposed related mechanisms to protect privacy by limiting the overall number of law enforcement searches and seizures. *Cf.* Kiel Brennan-Marquez & Stephen E. Henderson, *Search and Seizure Budgets* (2022) (on file with author), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3910743 [https://perma.cc/SQ8G-WVRY] (proposing a cap on the number of searches and seizures police may perform per year as a mechanism for limiting police intrusions into the lives of citizens).

1. Jurisdictional Challenges

As to the first kind of challenge, multiple pro-choice states have issued orders barring law enforcement agencies within that state from cooperating with out-of-state restrictionist investigations.[317] For instance, the Governor of Massachusetts has specifically prohibited the state's law enforcement agencies from executing out-of-state restrictionist arrest warrants.[318] The Governor of Washington has prohibited the Washington State Patrol from cooperation with out-of-state warrants, subpoenas, and court orders seeking abortion-relevant data,[319] and local law enforcement agencies in Washington have followed suit.[320]

Technology companies could follow suit by adopting similar policies and refusing to comply with out-of-state antiabortion warrants, subpoenas, and court orders that have not been domesticated through the state courts for the state in which the company is headquartered. As we have explained,[321] most states have adopted some version of the Uniform Act and UIDDA to facilitate evidence gathering across state lines in both criminal and civil cases. But both of these regulatory structures generally require that a court in the recipient's state review the out-of-state legal process and issue a local order to enforce it.[322] Courts in the recipient's state have some discretion as to whether or not to issue such an enforcement order. Technology companies can attempt to persuade courts within their own states not to enforce antiabortion legal processes by arguing that compliance would be unreasonable and unduly burdensome.[323]

---

317 *See, e.g.*, Dialynn Dwyer, *Charlie Baker Signs Executive Order to 'Further Preserve' Abortion Rights, Protect Providers in Mass.*, BOSTON.COM (June 24, 2022), https://www.boston.com/news/politics/2022/06/24/baker-executive-order-protect-reproductive-health-care-services [https://perma.cc/2ZVE-X3UT].

318 *Id.*

319 Directive of the Governor, from Governor Jay Inslee to The Washington State Patrol (June 30, 2022), https://www.governor.wa.gov/sites/default/files/directive/22-12%20-%20Prohibiting%20assistance%20with%20interstate%20abortion%20investigations%20(tmp).pdf?utm_medium=email&utm_source=govdelivery [https://perma.cc/KY3M-DAZA].

320 *WA Sheriff Won't Cooperate With Out-of-State Abortion Probes*, AP NEWS (July 5, 2022), https://apnews.com/article/abortion-health-seattle-washington-jay-inslee-0e1d3fa54a928ca5f0dfbcb753a50139 [https://perma.cc/86F5-F7VE].

321 *See supra* text accompanying notes 217–23.

322 *See, e.g.*, White II, *supra* note 218.

323 *See, e.g.*, O'Donnell v. Cooper Tire & Rubber Co., 2016 WL 4036887, at *8 (Ohio Ct. App. 2016) (affirming that courts in a discovery state have an "interest in protecting its residents from unreasonably and overly burdensome discovery requests" via out-of-state subpoenas); Hyatt v. State Franchise Tax Bd., 105 A.D.3d 186, 200–01 (N.Y. App. Div. 2013) (observing that discovery via subpoena "must comply with the rules of the state in which it occurs," and that "the discovery state has a significant interest in protecting its

2. *Substantive Challenges*

If the jurisdictional challenge fails, a next step should be the filing of a substantive motion to quash. For instance, warrants can be challenged for their overbreadth or lack of particularity.[324] Subpoenas can be challenged as unduly burdensome due to the costs of compliance or the level of privacy intrusiveness.[325] Major technology companies have filed motions to quash warrants and subpoenas in the past, challenging both the scope and validity of legal process. They have done so, importantly, prior to disclosing any responsive data. As recently as April 2022, Facebook filed a motion to quash a warrant in a white-collar criminal case in New Jersey—and won.[326] Firms have also successfully challenged subpoenas from nongovernmental litigants and won, without ever having to hand over the requested data.[327] Even the risk of having to litigate against a well-resourced technology company filing a motion to quash could chill or slow down antiabortion regulators from seeking data disclosures.

3. *Nondisclosure Orders*

Finally, many technology companies have undertaken contractual obligations to notify users when their information is the target of legal process.[328] Firms that have not yet undertaken these obligations should do so, and all firms should prioritize notice to users regarding

---

residents who become non-party witnesses in an action pending in another jurisdiction from unreasonable or burdensome discovery requests" (quoting ADVISORY COMM. ON CIVIL PRAC., REPORT TO THE CHIEF ADMINISTRATIVE JUDGE OF THE COURTS OF THE STATE OF NEW YORK 26 (Jan. 2009)).

[324] *Cf.* Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 IOWA L. REV. 1643, 1651–56 (2020) (arguing that existing limits on "uncommonly broad" digital searches are inadequate and proposing an inventory requirement to limit the ex post use of data seized through such searches); Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 EMORY L.J. 49, 52–55 (2018) (proposing minimization requirements as a solution to the inevitable overbreadth of digital searches); Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 11–12 (2011) (responding to Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (Oct. 2010) (debating authority of magistrate judges to issue minimization requirements for digital searches).

[325] *See, e.g.*, Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 U.C.L.A. L. REV. 212, 226 (2021) (describing judicial discretion to quash subpoenas that are "unreasonable or oppressive" (quoting FED. R. CRIM. P. 17(c)(1)–(2)).

[326] Facebook, Inc. v. State, 273 A.3d 958 (N.J. Super. Ct. A.D. 2022).

[327] *See, e.g.*, Facebook, Inc. v. Wint, 199 A.3d 625, 626 (D.C. 2019).

[328] *See, e.g.*, *Information for Law Enforcement Authorities*, FACEBOOK, https://www.Facebook.com/safety/groups/law/guidelines [https://perma.cc/E4FK-CR2Y]; *Cloudflare Transparency Report*, CLOUDFLARE, https://www.cloudflare.com/transparency [https://perma.cc/L697-ZY7K]; *Legal Request FAQs*, TWITTER, https://help.twitter.com/en/rules-and-policies/twitter-legal-faqs [https://perma.cc/8TCG-EW32]; *see also* Sharon D. Nelson

legal process demands for abortion-relevant data. Notice matters most obviously because it enables the actual target of the investigation to assert their privacy rights and mount legal challenges to the scope and validity of the legal process in court.[329] But notice also matters for a more subtle reason: It can help to combat law enforcement use of parallel construction to conceal potentially unlawful or unconstitutional investigative methods from the courts.[330]

To be sure, sometimes firms are prohibited from providing such notice by nondisclosure orders, otherwise known as gag orders, that accompany legal process seeking sensitive user data.[331] But technology firms also have a well-established history of challenging such gag orders.[332] Major firms have mounted successful First Amendment challenges to gag orders accompanying National Security Letters or FBI administrative subpoenas.[333] Following litigation on these issues, Congress changed the National Security Letter statutes to establish procedures for adversarial judicial review of the gag orders.[334] And currently, Congress is considering the Nondisclosure Order (NDO) Fairness Act, which would require law enforcement to meet new and

& John W. Simek, *How to Protect Data from Uncle Sam*, LITIGATION, Fall 2014, at 11, 12 (noting that smaller tech firms are more likely to hand over data).

329 *See generally* Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843, 851 (2015) (explaining that notice is justified by "a privacy interest that all individuals share" and "the principle that, when the government chooses to prosecute an individual on the basis of evidence obtained through a Fourth Amendment search, the defendant must be able to test whether the government obtained its evidence lawfully").

330 *See generally* Natasha Babazadeh, *Concealing Evidence: "Parallel Construction," Federal Investigations, and the Constitution*, 22 VA. J.L. & TECH. 1, 1 (2018) ("Parallel construction is the process of building a separate—and parallel—evidentiary basis for a criminal investigation. The process is undertaken to conceal the original source of evidence, which may have been obtained unlawfully.").

331 *See, e.g.*, 18 U.S.C. § 2705(b) (SCA gag order provision).

332 *See, e.g.*, Brad Smith, *DOJ Acts to Curb the Overuse of Secrecy Orders. Now It's Congress' Turn*, MICROSOFT: MICROSOFT ON THE ISSUES (Oct. 23, 2017), https://blogs.microsoft.com/on-the-issues/2017/10/23/doj-acts-curb-overuse-secrecy-orders-now-congress-turn [https://perma.cc/A6NL-3V2L] (describing a Microsoft challenge to government gag orders for data requests under the Stored Communications Act). Indeed, Microsoft has challenged the legality of the standard procedures applied in contestation over gag orders. Cyrus Farivar, *DOJ Changes "Gag Order" Policy, Microsoft to Drop Lawsuit*, ARSTECHNICA (Oct. 24, 2017, 5:12 AM), https://arstechnica.com/tech-policy/2017/10/doj-changes-gag-order-policy-microsoft-to-drop-lawsuit [https://perma.cc/YW2F-HXBN].

333 *See, e.g.*, *In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064, 1066–67 (N.D. Cal. 2013); *see also FBI Withdraws Unconstitutional National Security Letter After ACLU and EFF Challenge: Gag Order Lifted on Internet Archive, Allowing Founder to Speak Out for First Time*, ELEC. FRONTIER FOUND., (May 6, 2008), https://www.eff.org/press/archives/2008/05/06 [https://perma.cc/97CZ-G7U6] (describing successful challenge to gag order by the ACLU and Electronic Frontier Foundation).

334 18 U.S.C. § 3511.

more rigorous standards in court to establish that secrecy is necessary before obtaining a gag order, would ban indefinite gag orders, and would mandate notice to the targeted user within seventy-two hours after the gag expires.[335] The NDO Fairness Act has already passed the House and is under consideration in the Senate. If the Act becomes law, it will create a legal framework for challenges to gag orders in court. Tech companies should double down on their track records of contesting the existence, scope, and duration of gag orders—particularly those accompanying legal process that targets abortion-relevant data.

4. Distinguishing Antiabortion Investigations

But does not the foregoing assume that technology companies will know which law enforcement requests pertain to antiabortion prosecutions or civil suits and which pertain to unrelated urgent investigations into, for instance, murder, domestic violence, child exploitation, or domestic terrorism? How, in practice, can that distinction be made, especially given the incentive of restrictionist prosecutors to obscure their motives? Certainly, a policy of non-cooperation with every law enforcement request would impose undesirable personnel and legal costs on companies with normatively undesirable collateral harms to law enforcement investigations across the board. Companies need the ability to segment out antiabortion investigations for special treatment. But how should they do so?

There are a number of ways that companies could achieve the necessary segmentation. As mentioned above, companies could use their existing tiered portal systems to incentivize law enforcement to disclose further relevant details about the type of crime under investigation. Given the incentive to obscure the connections between a prosecution and reproductive choice, a company could place the burden on the state to show that no such connection exists. All legal process could, by default, go through the second-tier, inefficient system, but law enforcement could seek to upgrade to the top-tier, efficient portals by certifying, and perhaps even demonstrating that they are not engaged in an antiabortion investigation or prosecution.

In addition, human reviewers at the companies often engage in an informal negotiation process with law enforcement requesters that determines the scope of the company's response. As Yan Fang has shown, reviewers may end up producing something narrower than

[335] N.D.O. Fairness Act, H.R. 7072, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/7072 [https://perma.cc/X9FA-KXBP] (reporting passage in the House of Representatives).

what the language in a warrant literally demands, and in doing so the reviewers necessarily make choices based on interpreting what they think is relevant to the warrant and hence to the purpose of the investigation.[336] As part of that process, reviewers sometimes converse with the law enforcement requester to try to gauge what crimes the investigation really focuses upon, and also whether it is a serious request or perhaps just an attempt to "fish[]" for data.[337] Reviewers engaged in those negotiations could simultaneously attempt to discern whether the requester is pursuing an antiabortion investigation.

Finally, some jurisdictions, including federal courts, require that warrants list the specific criminal statutes that have allegedly been violated, which may tell receiving companies if the warrant pertains to an antiabortion investigation.[338] More such requirements could be written into law for both warrants and subpoenas. Most obviously, pro-choice states could pass statutes prohibiting their courts from enforcing out-of-state legal process unless the warrant or subpoena indicates the conduct under investigation.

D. Enabling Individual Choice Through Private and Secure Access to Accurate Information

Even without active resistance to legal process demands, the technological infrastructure that firms provide to their users can expand or restrict reproductive privacy and choice. Beyond enabling or throttling access to accurate information to facilitate a patient's search for care, as discussed above,[339] firms can also provide more and less privacy-protective options for searching that information. For instance, some but not all currently offer end-to-end encryption by default for all communications.[340] In the wake of *Dobbs*, digital civil

---

336 *See* Fang, *supra* note 308, at 23–25.

337 *Id.* at 25.

338 To be sure, some antiabortion prosecutions have already been brought using child endangerment statutes, so law enforcement could conceivably conceal their purpose by listing an alternative charge on the warrant. *See* Noa Yachot, *Who Will Be Prosecuted for Abortion if Fetuses Are Recognized as People?*, THE GUARDIAN (May 18, 2022, 5:00 AM), https://www.theguardian.com/law/2022/may/18/abortion-prosecution-fetal-homicide-law [https://perma.cc/L8YQ-62RF]. Tech firms could ask prosecutors, though, to list all reasonably foreseeable offenses that could be charged in relation to the underlying conduct.

339 *See supra* text accompanying notes 79–90.

340 *See* Ken Kantzer, *Yet Another End-to-End Encrypted App*, PKC SECURITY (Dec. 16, 2016), https://blog.balboa.io/yet-another.html [https://perma.cc/NGS4-7LAN] ("It seems that every week, yet another end-to-end encrypted app is unleashed on the world."); Leonid Grinberg, *End-to-End Authentication: A First Amendment Hook to the Encryption Debate*, 74 N.Y.U. ANN. SURV. AM. L. 173, 174 (2018) ("The past few years have seen a proliferation of messaging services offering 'end-to-end encryption.'"). In contrast, Twitter

liberties organizations jumped to provide advice to pregnant people on how to navigate the digital ecosystem safely, including segmenting abortion-relevant data from other activities, selecting alternate privacy-protective browsers, and using a "burner phone," encryption, and secure deletion of sensitive files.[341] While such guides are helpful interventions, they do not empower all users equally. Most of those who are vulnerable to state regulation are low income and often members of marginalized racial and ethnic minorities.[342] They may not have the time or resources to invest in researching and implementing privacy precautions. A key question is how best to empower those especially vulnerable users.

We propose a technological intervention to facilitate and enlarge personal choice specifically for such users: a bot that operates on social media platforms to guide people through privacy protection steps and steps needed to acquire and use information. A social media bot is a program, often built on artificial intelligence, that can "talk to [people] through technology that was designed for humans to talk to humans."[343] Some platforms, including Instagram, restrict the use of bots; others, including TikTok—a platform especially popular with young women[344]—do not.[345] A bot on TikTok can be given "target audience guidelines and custom filters which it then uses to automate the activity of liking, commenting, and following other account[s'] posts and profiles at scale."[346] At present, bots are often used to generate comments on postings to simulate (and stimulate) user engagement. They can also intervene by posting content if specific hashtags

---

and Gmail do not. Importantly, even end-to-end encryption does not shield metadata, so using such services may still leave pregnant patients vulnerable.

341 Daly Barnett, *Security and Privacy Tips for People Seeking an Abortion*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (June 23, 2022), https://www.eff.org/deeplinks/2022/06/security-and-privacy-tips-people-seeking-abortion [https://perma.cc/97CZ-G7U6].

342 *See* Leah Litman, *Redefining Reproductive Rights and Justice*, 118 MICH. L. REV. 1095, 1104 (2020) (noting these disparate effects).

343 Mike Simpson, *Social Media Bots: How They Work and How to Use Them*, MELTWATER (Mar. 19, 2021) (alteration in original), https://www.meltwater.com/en/blog/social-media-bots [https://perma.cc/J7Y3-34V5]; *see also* DEP'T OF HOMELAND SEC., OFF. OF CYBER & INFRASTRUCTURE ANALYSIS, SOCIAL MEDIA BOTS OVERVIEW 1 (May 2018), https://niccs.cisa.gov/sites/default/files/documents/pdf/ncsam_socialmediabotsoverview_508.pdf?trackDocs=NCsam_socialmediabotsoverview_508.pdf [https://perma.cc/F2Q3-779F] (describing types of attack by social media bots).

344 Fifty-seven percent of TikTok users are women. Josh Howarth, *TikTok User Age, Gender, & Demographics (2022)*, EXPLODING TOPICS (Jan. 13, 2023), https://explodingtopics.com/blog/tiktok-demographics [https://perma.cc/LTP7-86LN].

345 Eduardo Morales, *TikTok Bots–The Best & Safest Options in 2022*, BETTER MKTG. (May 12, 2020) https://bettermarketing.pub/tiktok-bots-the-best-bot-providers-ca6ebe9a0134 [https://perma.cc/8SN3-JTNJ].

346 *Id.*

are trending. They can even conduct simple conversations, via posts and replies, with human users. In the reproductive health space, some healthcare providers are eager to employ such chat bots to supply basic information.[347] One app, MedChat, allows users to "configure what interactions would require patients to identify themselves and which would not."[348]

We would take the idea of a bot one step further and propose a more proactive social-media intervention. This idea draws inspiration from an innovation pioneered by an organization called Women on Waves, which uses a bot to deliver medication abortion in Northern Ireland and Poland.[349] The intervention would seek out and guide pregnant persons through the necessary precautions to securely use digital services to minimize locational- or biometric-data trails and to obtain accurate medical information and unvarnished accounts of their options and legal risks. Such a bot, for example, might first be designed to help a pregnant person configure a browser to maximize privacy. It would thus create no digital record either in a central database or in a user's device. It might even guide them through the installation of Tor, an application that shields a user's IP address and allows them to surf anonymously.[350] It would then navigate toward truthful, helpful information about abortion access. It could even offer personalized abortion-related information through an automated chat

---

[347] Brit Morse, *With* Roe v. Wade *on the Chopping Block, Companies Count on Chatbots to Fill the Reproductive Care Void*, INC. (June 22, 2022), https://www.inc.com/brit-morse/healthcare-providers-abortion-rights-chatbots-messaging-platforms-laws.html [https://perma.cc/2TUE-3TEF].

[348] *Id.*

[349] *Abortion Robots*, WOMEN ON WAVES, https://www.womenonwaves.org/en/page/7524/abortion-robots [https://perma.cc/N55P-PCXB].

[350] Tor is short for "The Onion Router": It enables users to engage on the internet anonymously. KRISTIN FINKLEA, CONG. RSCH. SERV., R44101, DARK WEB 3–4 (2017), https://fas.org/sgp/crs/misc/R44101.pdf [https://perma.cc/7ZRM-MX37]. "Tor" describes both the software that users install on their devices to operate anonymously, *id.*, and the collection of "volunteer-operated servers" that support the Tor network. *Tor: Overview*, TOR, https://2019.www.torproject.org/about/overview.html.en [https://perma.cc/4GV2-ACZ7]. Tor conceals a user's IP address by routing web traffic through a series of relays, or nodes, run by these servers. Information is encrypted between relays and takes on the IP address of the final "exit" relay. I2P, or the Invisible Internet Project, is another popular anonymous network. Tor recently played a role in helping Iranian protestors stay online securely. *See, e.g.*, Mike Butcher, *As Iran Throttles Its Internet, Activists Fight to Get Online*, YAHOO! (Oct. 5, 2022), https://www.yahoo.com/now/iranian-tech-activists-detail-tech-161327435.html [https://perma.cc/V7ZQ-XX6K]. There have been previous *human* efforts to disseminate information about using Tor; using a bot to the same end is a logical extension of these efforts. *See* Richard Esguerra, *Help Protesters in Iran: Run a Tor Bridge or a Tor Relay*, ELEC. FRONTIER FOUND. (June 29, 2009), https://www.eff.org/deeplinks/2009/06/help-protesters-iran-run-tor-relays-bridges [https://perma.cc/2AET-447K] (encouraging volunteers to configure their computers as a Tor bridge to support Iranian protestors attempting to access the internet).

function, as MedChat does. Like the customer service bots that are already used by banks and airlines, such a bot could use the location and financial situation of a user to tailor quite specific courses of action.

The virtue of this kind of intervention—which, we note, could be launched and maintained from anywhere, including outside the United States—is that it would target precisely those demographics that are most in need. Many of those most vulnerable to state coercion for their reproductive choices are likely to be users of platforms like TikTok—recall the users skew young and female.[351] Reaching them through a well-designed bot would minimize legal risks from restrictionist state legislation, while maximizing both privacy and effectual choice.

E. A New Evidentiary Privilege for Reproductive Choice

Although technology companies currently have vast discretion in how to respond to law enforcement and vigilante service of legal process, there is an important opportunity for legislators to impose legal restrictions to force companies to do the right thing—and for companies to lobby for the same. To date, many of the legislative efforts to shield abortion-relevant data from the reach of restrictionist law enforcement and vigilantes have focused on limiting interjurisdictional cooperation among law enforcement[352] and enacting information privacy statutes.[353] This approach falls short because courts may still facilitate cross-jurisdictional evidence collection even without assistance from local law enforcement, and privacy statutes generally offer no protection from compulsory legal process.[354] For instance, the My Body, My Data Act of 2022 would restrict technology companies' voluntary collection, retention, use, and disclosure of "personal reproductive or sexual health information," but the Act does not block, or

---

[351] *See* Howarth, *supra* note 344 (noting that one in four TikTok users are under twenty-years-old and fifty-seven percent of TikTok users are female).

[352] *See* Cohen, Donley & Rebouché, *supra* note 193, at 13–26 (discussing cross-border abortion liability).

[353] *See, e.g.*, My Body, My Data Act of 2022, H.R. 8111, 117th Cong. (2022) (protecting collection, retention, use, and disclosure of personal reproductive and sexual health information); *see also* Health and Location Data Protection Act of 2022, S. 4408, 117th Cong. (2022) (protecting personal location and health data); Cameron F. Kerry, *How Comprehensive Privacy Legislation Can Guard Reproductive Privacy*, BROOKINGS INST. (July 7, 2022), https://www.brookings.edu/blog/techtank/2022/07/07/how-comprehensive-privacy-legislation-can-guard-reproductive-privacy [https://perma.cc/7NRE-7VAZ] (discussing the American Privacy and Data Protection Act).

[354] *See supra* text accompanying notes 95–104.

indeed even mention, warrants, subpoenas, or other court orders.[355] Moreover, as detailed above, existing information privacy statutes that cover some abortion-relevant data, such as HIPAA and the Stored Communications Act, contain exceptions that expressly authorize disclosures pursuant to warrants, subpoenas, and other forms of compulsory process.[356]

Restrictionist states' post-*Dobbs* turn to the expansive criminal law and vigilante civil bounty statutes necessitates something more than a default rule of information privacy. It calls for a legislative response powerful enough to combat both law enforcement and judicial compulsory process. Fortunately, a well-established legal authority could bar the use of much abortion-relevant data in criminal or civil investigations, as well as pre-trial, trial, and post-trial proceedings, nationwide. This legal authority is drawn from evidentiary privilege law. We advocate that federal and state legislatures should enact statutory evidentiary privileges that not only protect abortion-relevant data from voluntary disclosure but also make that data immune from law enforcement and judicial compulsory legal process alike.

The concept of evidentiary privilege protections for abortion-relevant data was first introduced publicly by one of us in testimony before the Judiciary Committee for the U.S. House of Representatives on July 19, 2022.[357] We lay out here the scholarly and doctrinal bases behind this proposal, which might be adopted not just at the federal level but could also be usefully adopted in pro-choice states. In the

---

[355] My Body, My Data Act of 2022, S. 4434, 117th Cong. (2022); My Body, My Data Act of 2022, H.R. 8111, 117th Cong. (2022). Similarly, the Fourth Amendment Is Not For Sale Act would prohibit law enforcement and intelligence agencies from circumventing the warrant requirement by purchasing Fourth Amendment-protected data, including abortion-relevant data, on the open commercial market, but the Act provides no protection against warrants or indeed against any other form of legal process applied to the majority of abortion-relevant data that does not fall within existing Fourth Amendment doctrine. Fourth Amendment Is Not For Sale Act, H.R. 2738, 117th Cong. (2021). Meanwhile, other legislative proposals seek to prohibit interference with the provision of abortion services but do not address data protection issues at all. *See, e.g.*, Ensuring Access to Abortion Act of 2022, H.R. 8297, 117th Cong. (2022); *see also* Women's Health Protection Act of 2022, H.R. 8296, 117th Cong. (2022).

[356] *See, e.g.*, 18 U.S.C. § 2703(b)–(c); *see also* 45 C.F.R. § 164.512(e)–(f); *cf.* United States v. Warshak, 631 F.3d 266, 282–88 (6th Cir. 2010) (applying the Fourth Amendment to stored electronic communications contents and thus presuming that law enforcement can seize such information using a probable cause warrant).

[357] *Digital Dragnets: Examining the Government's Access to Your Personal Data: Hearing Before the H. Comm. on the Judiciary*, 117th Cong. (2022) (statement of Rebecca Wexler); House Committee on the Judiciary, *Digital Dragnets: Examining the Government's Access to Your Personal Data*, YOUTUBE, at 02:30:00 (July 19, 2022), https://www.youtube.com/watch?v=F27nOcsenRY&ab_channel=HouseCommitteeontheJudiciary [https://perma.cc/WXQ2-M49S].

Appendix, we offer a model bill text that federal and pro-choice state lawmakers can use to create an abortion data evidentiary privilege.

It is helpful to begin by explaining the extraordinary power of evidentiary privileges in general.[358] Not only do privileges bar protected information from being admitted into evidence at trial, but—unlike any other evidence rule—they also preclude the use of protected information at all other stages of a judicial proceeding.[359] That means privileges do not just bar juries from considering protected information; they also bar judges from doing so.[360] Privileges also apply to bail hearings, settlement agreements, plea negotiations, sentencing proceedings, and more.[361] Further, they prevent litigants, including criminal prosecutors and vigilante civil plaintiffs, from ever learning the information in the first place. Privileges have the power to block or prevent the use of evidence gained through subpoenas,[362] discovery orders,[363] searches and seizures,[364] and even wiretaps.[365] This is so regardless of probable cause and ex ante judicial review. In other words, privileges offer more powerful privacy protections than even the Fourth Amendment—which provides minimal safeguards when the government can show probable cause or reasonable suspicion.[366]

---

358 EDWARD J. IMWINKELRIED, THE NEW WIGMORE: A TREATISE ON EVIDENCE: EVIDENTIARY PRIVILEGES 3 (Richard D. Friedman ed., 2d ed. 2010) ("[P]rivileges are the evidentiary rules that allow a person [or legal entity] who communicated in confidence or who possesses confidential information to shield the communication or information from compelled disclosure during litigation." (footnote omitted)).

359 *See, e.g.*, FED. R. EVID. 1101(c) ("The rules on privilege apply to all stages of a case or proceeding.").

360 *See id.* at 1101(c)–(d) (stating that exceptions to evidentiary rules do not apply to evidentiary privileges).

361 *See id.* at 1101(b) (providing that privilege rules apply in civil cases and proceedings, criminal cases and proceedings, and contempt proceedings).

362 *See* FED. R. CIV. P. 45(d)(3)(A)(iii) (providing that the court must quash or modify a subpoena that requires disclosure of privileged information).

363 *See* FED. R. CRIM. P. 17(c); *see also* Bowman Dairy Co. v. United States, 341 U.S. 214, 221 (1951); United States v. Iozia, 13 F.R.D. 335, 338 (S.D.N.Y. 1952).

364 *See* 18 U.S.C. § 2517(4) (stating that a seized communication does not lose its privileged character); *see also* Eric D. McArthur, Comment, *The Search and Seizure of Privileged Attorney-Client Communications*, 72 U. CHI. L. REV. 729, 740–44 (2005) (discussing case law suggesting that privileged attorney-client communications cannot be searched and seized).

365 18 U.S.C. § 2517(4).

366 *See* Elizabeth E. Joh, *Fourth Amendment Rights as Abortion Rights*, N.Y.U. L. REV. F. (Oct. 24, 2022), https://www.nyulawreview.org/forum/2022/10/fourth-amendment-rights-as-abortion-rights [https://perma.cc/G6HT-AVQW] (explaining that existing Fourth Amendment doctrine will fail to shield abortion seekers from informants, *Terry* stops, and pretextual policing); *see also* Elizabeth Joh, *The Potential Overturn of* Roe *Shows Why We Need More Digital Privacy Protections*, SLATE: FUTURE TENSE (May 9, 2022, 2:02 PM) https://slate.com/technology/2022/05/roe-overturn-data-privacy-laws.html [https://perma.cc/

We envision an abortion data privilege that would be jointly held by any person seeking, obtaining, providing, or assisting in seeking, obtaining, or providing abortion services. All joint holders of the privilege would be required to waive the privilege before protected information could be used in court. Further, this should be a topical privilege, such as the trade secret[367] or state secret privileges.[368] This echoes a proposal by Jerry Kang and co-authors for a "self-surveillance privilege" that would "protect the self-surveillance data stored in [a firm that collected such data]."[369] Similar to the self-tracking data described *supra*,[370] Kang and co-authors define "self-surveillance data" as "measurements of the individual self, initiated by the self, using sensors that are in one's control, for the primary purpose of measuring the self."[371] Data subject to that proposed self-surveillance privilege could not "be subpoenaed or introduced into any legal proceeding unless the privilege was waived by the individual or subject to some clearly delimited exception."[372] Similarly, with an abortion data privilege, anyone in possession of abortion-relevant data would be required to assert the privilege absent waiver by all of the joint holders.[373]

Moreover, we advocate that the abortion data privilege should include no statutory exceptions and should expressly preclude court-created or common-law exceptions. This absolutism diverges from standard privilege practice. Some evidentiary privileges are explicitly qualified and subject to balancing against countervailing interests in accessing protected information.[374] Yet even those privileges that are facially absolute generally have particularized exceptions for circumstances such as self-defense, child abuse prosecutions, and disclosures of an ongoing or future crime or fraud.[375] For instance, both the existing trade secret evidentiary privilege and the self-surveillance

4A29-6Q6W] (explaining that the post-*Carpenter* Fourth Amendment offers uncertain protection for records in the hands of a third party, and that police can circumvent the warrant requirement by purchasing data in commercial markets).

367 *See, e.g.*, CAL. EVID. CODE § 1060 (West 2022) (stating California's trade secret privilege).

368 *See* United States v. Reynolds, 345 U.S. 1, 6–10 (1953) (establishing modern state secret privilege).

369 Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke & Mark Hansen, *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 832, 835 (2012).

370 *See supra* Section I.B (describing self-tracking).

371 Kang et al., *supra* note 369, at 814 (footnote omitted).

372 *Id.* at 832.

373 *Cf.* IMWINKELRIED, *supra* note 358, at 1391–1483 (discussing procedures for asserting and waiving state secret privilege and trade secret privilege).

374 *See id.* at 1470–73 (explaining that trade secret privilege is a qualified privilege).

375 *See generally id.* at 1141–70 (discussing exceptions for privileges).

privilege proposed by Kang and coauthors would not apply if their allowance would "tend to conceal fraud, enable criminal activity or otherwise work injustice."[376] Similarly, in many states the attorney-client privilege authorizes disclosures to prevent "reasonably certain death or substantial bodily harm."[377] The problem with including such exceptions in an abortion data privilege is that it would create a loophole for restrictionist courts to find that the privilege does not apply in antiabortion proceedings.[378]

At the same time, we are sensitive to the risk that a truly absolute privilege might cause unintended, harmful consequences. As a result, we propose an extraordinarily narrow application for the privilege. The privilege should apply solely to proceedings to hold a person criminally or civilly liable for seeking, obtaining, providing, or assisting in seeking, obtaining, or providing abortion services. In other words, when it comes to medical liability disputes, domestic violence cases, child abuse prosecutions, or any other form of litigation, this privilege would not apply at all. While unusual, such a narrow application for a statutory privilege is not unprecedented.[379] It has indeed been upheld by the Supreme Court.[380]

The main area for policymakers to exercise discretion in implementing our proposal is the scope of information to be covered by the abortion data privilege. Given the extremely narrow application of the privilege solely to abortion-related litigation, we advocate for as broad coverage as possible. An example would be coverage for: all data that reveals a person's efforts to seek, obtain, provide, or assist in seeking, obtaining, or providing abortion services, including but not limited to healthcare and insurance records pertaining to abortion services; communications between a pregnant person and others for the purposes

---

376 Kang et al., *supra* note 369, at 834.

377 MODEL RULES OF PRO. CONDUCT r. 1.6(b)(1) (AM. BAR ASS'N 2019); *see also* Colin Miller, Colloquy, *Ordeal by Innocence: Why There Should Be a Wrongful Incarceration/Execution Exception to Attorney-Client Confidentiality*, 102 NW. U. L. REV. COLLOQUY 391, 394–95 (2008) (discussing adoption of Model Rule 1.6(b)(1) and ultimately arguing to extend the exception to permit disclosures that prevent wrongful incarceration and execution).

378 *Cf.* Chris Mills Rodrigo, *Amazon Admits to Giving Ring Videos to Police Without Permission*, THE HILL (July 13, 2022, 12:27 PM), https://thehill.com/policy/technology/3557545-amazon-admits-to-giving-ring-videos-to-police-without-permission [https://perma.cc/R4QU-S7UM] (reporting Amazon's use of the emergency exception in a privacy statute to disclose data to police).

379 There exists a federal statutory privilege that similarly applies solely to a small subset of narrowly defined cases. *See* 23 U.S.C. § 407 (creating a privilege that applies solely "in any action for damages arising from any occurrence at a location mentioned or addressed in [a highway safety survey]").

380 *See* Pierce Cnty. v. Guillen, 537 U.S. 129, 146 (2003) (upholding the constitutionality of 23 U.S.C. § 409, now codified at 23 U.S.C. § 407).

of obtaining abortion care or information about abortion care; commercial transactional records concerning abortion services; biometric data revealing the presence or absence of pregnancy or abortion; geolocation data concerning abortion service providers; and data pertaining to internet or other searches associated with abortion services.

Notably, there are no clear limits on the scope of information that a legislature can protect with a privilege.[381] Rather than ex ante bounds on scope, the limits on legislative authority in this domain derive from individual litigants' as-applied constitutional rights. As with all privileges, opposing litigants may be able to pierce the privilege on a case-by-case basis if they can establish a conflicting constitutional need to access the protected information, such as a criminal defendant's Sixth Amendment right to compulsory process or a civil litigant's Fifth and Fourteenth Amendment rights to due process.[382] Thus, legislators need not worry about extending the scope of coverage broadly at the outset.

Ideally, the U.S. Congress would enact an abortion data privilege that applies nationwide. No one doubts that states can create statutory evidentiary privileges. Less commonly known, the federal government also has uncontroverted power to enact statutory evidentiary privileges, including ones that apply in state as well as in federal court.[383] Although the Federal Rules of Evidence left privileges primarily to the development of the common law, Rule 501 reserved authority for the U.S. Congress to enact statutory evidentiary privileges.[384] There are hence a number of federal statutory privileges.[385] For one example, statutory text stating expressly that information "shall be immune from legal process" creates a facially absolute evidentiary privilege that blocks all forms of compulsory legal process, including

---

381 For instance, while existing federal statutes generally privilege information possessed by governmental entities, some also extend to information possessed by private individuals and entities. *See, e.g.*, 13 U.S.C. § 9(a)(3) ("Copies of census reports which have been so retained [by private establishments or individuals] shall be immune from legal process, and shall not . . . be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding.").

382 *See* Edward J. Imwinkelried, *Questioning the Behavioral Assumption Underlying Wigmorean Absolutism in the Law of Evidentiary Privileges*, 65 U. PITT. L. REV. 145, 162–63 (2004) ("[I]n the United States even purportedly absolute privileges are already qualified . . . because criminal accused and civil litigants have a constitutional right to surmount the privilege in order to introduce critical, demonstrably reliable evidence.").

383 *See* Natalie Ram, Jorge L. Contreras, Laura M. Beskow & Leslie E. Wolf, Constitutional Confidentiality 32 (Sept. 1, 2022) (unpublished manuscript) (on file with authors) (explaining that the federal Certificates statute creates an evidentiary privilege that applies in state as well as federal court).

384 FED. R. EVID. 501.

385 *See, e.g.*, Mila Sohoni, *The Power to Privilege*, 163 U. PA. L. REV. 487, 497–99 (2015) (discussing federal statutory privileges, though conceding they are rare).

both warrants and subpoenas.[386] Other common formulations of the textual language in federal privilege statutes include that protected information "shall not . . . be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding";[387] shall not be subject to "discovery or compulsory process";[388] "shall be immune from legal process and shall not be subject to subpoena or other discovery";[389] and shall be protected "to the extent the communication would be considered a privileged communication if it were between a taxpayer and an attorney."[390]

The Supreme Court has also affirmed Congress's power to enact privileges that control in state court. In *Pierce County v. Guillen*, the Court reviewed a federal statute that provided, in relevant part, that "[n]otwithstanding any other provision of law, [protected information] . . . shall not be subject to discovery or admitted into evidence in a Federal *or State* court proceeding or considered for other purposes in any action for damages . . . ."[391] In a unanimous ruling, the Court affirmed that the federal statute protecting information "from being discovered or admitted in certain federal or state trials, is a valid exercise of Congress' authority under the Constitution."[392]

The U.S. Congress should enact a similarly express and facially absolute statutory evidentiary privilege in respect to abortion-relevant information.[393] As with the statutory privilege upheld in *Guillen*, an abortion data privilege would arguably fall within Congress's Commerce Clause authority.[394] Congress has long regulated the collection, storage, and disclosure of sensitive communications and health data.[395] As in *Guillen*, "Congress could reasonably believe that adopting a measure eliminating an unforeseen side effect of the information-gathering"—in this case the use of data as evidence in antiabortion investigations and judicial proceedings—would result in

386 13 U.S.C. § 9(a)(3); *see also* Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721, 2762–67 (2021) (discussing express statutory privileges).

387 13 U.S.C. § 9(a)(3).

388 5 U.S.C. § 574(a).

389 15 U.S.C. § 2055(e)(2).

390 26 U.S.C. § 7525(a).

391 Pierce County v. Guillen, 537 U.S. 129, 135–36 (2003) (emphasis added) (reviewing the constitutionality of 23 U.S.C. § 409, now codified at 23 U.S.C. § 407).

392 *Id.* at 132–33.

393 *Cf.* IMWINKELRIED, *supra* note 358, at 981–82 (discussing absolute communications privileges).

394 *Guillen*, 537 U.S. at 147.

395 *See, e.g.*, Stored Communications Act, 18 U.S.C. §§ 2701–12 (addressing disclosure of stored communications held by third-parties); *see also* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (stipulating standards for maintaining healthcare information).

"more diligent . . . better informed decisionmaking" concerning the use of electronic communications and healthcare services "and, ultimately, greater safety" for pregnant people and their care providers.[396]

Implementation of our proposal at the state level would look similar, albeit with the key difference that a state statutory privilege would apply solely to court proceedings in that state.[397] Hence, if the New York or Illinois legislatures enact a privilege, those privileges would immunize information solely from compulsory legal process issued by courts in New York or Illinois. Nonetheless, creating such a privilege in pro-choice states would still be valuable because it could bar courts in those states from enforcing cross-jurisdictional subpoenas, warrants, or other court orders that originate in restrictionist states.[398] And if an entity subject to the New York or Illinois privilege complied with an out-of-state antiabortion subpoena, the privilege

396 *Guillen*, 537 U.S. at 147.

397 *See* Baker v. Gen. Motors Corp., 522 U.S. 222, 239 (1998) ("[A] Michigan decree cannot determine evidentiary issues in a lawsuit brought by parties who were not subject to the jurisdiction of the Michigan court."). In diversity jurisdiction cases, federal courts apply the privilege law for the state in which they sit. *See* FED. R. EVID. 501 ("[I]n a civil case, state law governs privilege regarding a claim or defense for which state law supplies the rule of decision.").

398 As a general default rule, courts considering out-of-state legal process pursuant to the Uniform Act will defer to the privilege rules of the forum state. *See* RESTATEMENT (SECOND) OF CONFLICT OF L. § 139(1)-(2) (AM. L. INST. 1971) (stating that the admission of evidence will be governed by the privilege law of the jurisdiction trying the matter); *see also* Johnson v. O'Connor *ex rel.* Cnty. of Maricopa, 327 P.3d 218, 226 (Ariz. Ct. App. 2014) (holding that admissibility issues must be governed by the local law of the forum state); *see also* Holmes v. Winter, 3 N.E.3d 694, 707 (N.Y. 2013) ("[A]bsent a threatened violation of an extremely strong and clear public policy of this State . . . New York courts adjudicating CPL 640.10(2) applications should decline to resolve admissibility issues, including privilege claims, so that they can be decided in the demanding state."). However, some state courts have applied their own state's privilege law as a blocking statute that bars enforcement of out-of-state legal process, particularly when the privilege reflects strong public policy interests. *See, e.g.*, *id.* at 703–07 (refusing to issue a subpoena to send a New York witness to testify in a Colorado criminal proceeding because of New York State's journalistic privilege); *see also* People v. Marcy, 283 N.W.2d 754, 757 & n.4 (Mich. Ct. App. 1979) (refusing to issue a subpoena to send a Michigan witness to testify in a Delaware criminal proceeding because of Michigan's polygraph privilege). And where the law of the state is unclear, judges could consider privilege law when determining whether enforcing out-of-state legal process would impose an undue burden or hardship on their own state's resident. *Cf.* UNIF. ACT TO SECURE THE ATTENDANCE OF WITNESSES FROM WITHOUT A STATE IN CRIM. PROC., *supra* note 218, at § 2 (requiring a judge to determine that compelling a witness to testify in another state "will not cause undue hardship"). Applying an abortion data privilege to block cross-jurisdictional process from restrictionist states would be harmonious with the RESTATEMENT (SECOND) OF CONFLICT OF L. § 139(1)-(2) (AM. L. INST. 1971), which prioritizes admissibility in the event of a conflict between two states' privilege laws *unless* there is a "strong public policy" or "special reason" why evidence should not be admitted. An abortion data privilege in pro-choice states could certainly qualify as just such a strong public policy interest.

holders could potentially sue for violation of the privilege.[399] To date, the state of California has led the way in enacting the types of legislative protections that a privilege would afford. Specifically, on September 27, 2022, California modified its version of the UIDDA to bar California courts and lawyers from issuing subpoenas that seek information related to sexual and reproductive health for use in out-of-state antiabortion investigations.[400] California has also barred health care providers from disclosing "medical information related to an individual seeking or obtaining an abortion" to law enforcement or in response to subpoenas or requests based on out-of-state antiabortion investigations.[401] We think that these legislative steps are laudable, but more is likely needed. Enacting the abortion data privilege we suggest would expand these protections to more forms of data beyond medical information, such as locational information and social media communications.

Technology companies, we think, have an advocacy role to play in the creation of evidentiary privileges to protect information about abortion care. There are multiple reasons that firms should use their considerable lobbying heft to support efforts to enact these privileges. Among the ethical considerations discussed earlier in Section II.C, privilege protections fit especially neatly into firms' financial incentives to resist governmental (and other) demands for data. Not only do they protect the firm from being conscripted into an agent of law enforcement (or civil litigation), but they do so efficiently. Our proposed privilege protections would give firms a categorical shield to deny legal process demands without having to undertake the personnel and litigation costs of the jurisdictional, substantive, and nondisclosure order challenges proposed above in Section III.C. Prior commentators have made similar arguments in the past that categorical restrictions on responding to legal process are needed or else litigants "could flood companies with subpoenas."[402] Privileges would

---

399 *Cf.* Colleen K. Samson, *Causes of Action Against Physician or Other Health Care Practitioner for Wrongful Disclosure of Confidential Patient Information*, *in* 36 CAUSES OF ACTION § 1 (Richard J. Arneson ed., Thomas Reuters 2022) (discussing the cause of action for breach of doctor-patient confidentiality).

400 A.B. 2091, 2021–2022 Reg. Sess. (Cal. 2022); Adam Schwartz, *California Leads on Reproductive and Trans Health Data Privacy*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Oct. 1, 2022), https://www.eff.org/deeplinks/2022/09/california-leads-reproductive-and-trans-health-data-privacy [https://perma.cc/Z2QY-FFDZ].

401 A.B. 2091, 2021–2022 Reg. Sess. (Cal. 2022); *see also* Schwartz, *supra* note 400.

402 Trisha Thadani, *Defenders May Use Public Social Media Posts in Trial, Court Says*, S.F. CHRON. (May 24, 2018, 4:42 PM), https://www.sfchronicle.com/business/article/Defenders-mayuse-public-social-media-posts-in-12941962.php [https://perma.cc/D2X9-2YQJ].

provide firms with just such a categorical protection from a flood of restrictionist demands.

Conclusion

This Article has mapped the epistemic terrain of the coming wars over abortion-related digital privacy. It has explained the complex statutory and constitutional realities that will almost certainly enable restrictionist laws and enforcement actions to follow pregnant bodies across state lines. Laying out the groundwork of that tricky regulatory terrain exposes the impossibility of major technology firms protecting reproductive choice through either a myopic focus on their own employees or by segmenting their abortion policies state by state. Rather, the economic and normative imperative for firms in a post-*Dobbs* world is active resistance to restrictionist enforcement concerning all persons nationwide. This Article has detailed precise, concrete actions that firms can and should take to enact this resistance within the bounds of existing law, including non-collection and non-retention of abortion-relevant data; non-cooperation with restrictionist law enforcement and civil vigilante demands for data; technological interventions to empower the most vulnerable and least tech-savvy pregnant patients seeking reproductive care; and advocating for statutory evidentiary privileges that would make abortion-relevant data immune from legal process and entirely preclude its use in restrictionist criminal and civil prosecutions. There is no neutral ground for big tech post-*Dobbs*. Unless firms adopt the actions elucidated here, or similar interventions, they will be affirmative allies of the restrictionist project.

APPENDIX

Model Text for a State or Federal Abortion Data Evidentiary Privilege Bill

SECTION 1. PRIVILEGE ESTABLISHED.

a) DATA PRIVILEGE ESTABLISHED. Notwithstanding any other provision of law, abortion-relevant data [that affects interstate or foreign commerce or that is in the custody of any Federal officer or employee] shall be immune from legal process and shall not be subject to discovery, admitted into evidence, or considered for any other purpose in a proceeding referred to in subsection (b), without the consent of each person to whom the data pertains.

b) APPLICABLE PROCEEDINGS. A proceeding referred to in this subsection is any civil action or criminal prosecution before a State [or Federal] court, or any proceeding before a State [or Federal] agency, against a person for seeking, obtaining, providing, or assisting in seeking, obtaining, or providing abortion services.

c) SCOPE OF PRIVILEGE. No exception (including any exception for criminal fraud or public policy) to the application of subsection (a) to a proceeding referred to in subsection (b) shall exist, except as set forth in subsection (d).

d) EXCEPTION FOR PATIENTS. Subsection (a) does not apply to any proceeding brought by or on behalf of a person for whom abortion services are performed.

SEC. 2. DEFINITION.

In this Act:

a) The term "abortion services" means an abortion and any medical or non-medical services related to and provided in conjunction with an abortion (whether or not provided at the same time or on the same day as the abortion), including—
   1) Consultation services;
   2) Termination of a pregnancy before fetal viability; or
   3) Termination of a pregnancy after fetal viability if, in the good-faith medical judgment of the treating health care provider, continuation of the pregnancy would pose a risk to the pregnant patient's life or health.

b) The term "abortion-relevant data"—
   1) means data that either reveals or for which there is a meaningful risk that some combination of the data and other available data sources could be used to deduce, including through reidentification of previously anonymized data, a person's efforts to seek, obtain, provide, or assist in seeking, obtaining, or providing abortion services; and
   2) includes—
      a. healthcare and insurance records associated with abortion services;
      b. communications between a pregnant person and others for the purposes of obtaining or otherwise associated with abortion care or information about abortion care;
      c. other communications that reveal a person's efforts to seek, obtain, provide or assist in seeking, obtaining, or providing abortion services;
      d. commercial, transactional and other financial records associated with abortion services;
      e. biometric data associated with the presence or absence of pregnancy or abortion, including menstrual cycle tracking software and other health software data;
      f. geolocation data associated with abortion services; and
      g. data pertaining to internet or other searches associated with abortion services.

c) The term "health care provider" means any entity or individual (including any physician, certified nurse-midwife, nurse practitioner, and physician assistant) that—
   1) is engaged or seeks to engage in the delivery of health care services, including abortion services; and
   2) if required by law or regulation to be licensed or certified to engage in the delivery of such services—
      a. is so licensed or certified; or
      b. would be so licensed or certified but for a law, regulation, or other prohibition coming into effect on or after June 24, 2022, limiting the provision of abortion services.

d) The term "legal process" means any warrant, subpoena, discovery order, or other court order compelling disclosure of information.
e) The term "viability" means the point in a pregnancy at which, in the good faith medical judgment of the treating health care provider, based on the particular facts of the case before the health

care provider, there is a reasonable likelihood of sustained fetal survival outside the uterus with or without artificial support.

SEC. 3. RULE OF CONSTRUCTION.

a) NO EFFECT ON PROCEDURAL RULES. – Nothing in this Act may be construed to alter the operation of any rule of criminal or civil procedure, or any rule of evidence as those rules normally function in the absence of an evidentiary privilege.

b) NO EFFECT ON OTHER PROCEEDINGS. – Nothing in this Act may be construed to apply to a civil action, criminal prosecution, or administrative proceeding other than a proceeding referred to in subsection (b) of Section 1.