REPRODUCTIVE HEALTH CARE DATA FREE OR FOR SALE: POST-ROE SURVEILLANCE AND THE "THREE CORNERS" OF PRIVACY LEGISLATION NEEDED

Eunice Park*

Cite as: Eunice Park, *Reproductive Health Care Data Free or For Sale: Post-*Roe *Surveillance and the "Three Corners" of Privacy Legislation Needed*, 30 RICH. J.L. & TECH. 185 (2023).

* Associate Professor, Western State College of Law. I would like to thank the Future of Privacy Forum and its Advisory Board for awarding this paper the 13th Annual Privacy Papers for Policymakers Award in February 2023, and for providing a platform for sharing scholarship and ideas not only within, but also outside, the academy. The views expressed are my own. I dedicate this article to my mom, Kyung S. Park, and to the memory of my dad, Jong M. Park.

ABSTRACT

Conditions will be harsher now for women than before *Roe v. Wade* for one key reason: We live in a surveillance state. While reproductive health care will continue to be a political hot button, one way to manage some of the fallout from *Dobbs v. Jackson Women's Health Organization* is by placing over-due limits on state surveillance to protect the politically uncontroversial expectation of privacy for personal data. Specifically, measures are needed to protect the privacy of health care data, and, in particular, reproductive health care data. Currently, law enforcement can obtain such data not only through failings in existing legislation but also via the ample digital breadcrumbs that fall outside any regulatory construct, including data obtainable for "free" by subpoenas, orders, warrants, and geofence warrants; and data "for sale" by data brokers, including sensitive geolocation information and data from fertility apps.

Given the perfect storm of readily accessible troves of private digital information alongside a panoply of inconsistent state solutions, this Article urges that federal legislation is needed to provide privacy safeguards for reproductive health care data that provides "three corners" of protection in the digital era. The first corner defines health care data to include a specific carve-out for reproductive health care data. The second corner provides the substantive curb of prohibiting data brokers from selling this reproductive health care data. The third corner adds a necessary procedural protection: Because there is no other kind of health care data with the broad potential to subject a patient to criminalization, reproductive health care data that would not be obtainable without a warrant should not be admissible as evidence to criminalize the individual. Setting such a federal floor to limit law enforcement's ability to mine private data for evidence of abortion, criminalize women, and, disproportionately, criminalize women of color, is more critical than ever in the surveillance state.

I. INTRODUCTION

[1] Like the dystopia depicted in Margaret Atwood's *The Handmaid's Tale*,[1] the current political system is trending toward tyranny by a minority with diminished autonomy for the rest, especially women.[2] *Roe v. Wade* has been overturned, and further restrictions may await in the form of federal legislation banning abortion. If such legislation returns, conditions will be harsher for the women of today than they were in 1960[3] for one key reason: In the 21st century, we live in a surveillance state.[4] Whether illegal at a state or federal level, abortion will become a target for a law enforcement that has largely unregulated access to digital data.[5] A traditional warrant requires identifying a particular target in a particular investigation, but law enforcement does not need a warrant when it has unregulated options to subpoena or outright purchase the ample digital breadcrumbs that we all

[1] *See* MARGARET ATWOOD, THE HANDMAID'S TALE (Anchor Books 1998).

[2] *See* Jo Yurcaba, *Law professor Khiara Bridges calls Sen. Josh Hawley's questions about pregnancy 'transphobic'*, NBC NEWS (July 13, 2022, 1:47 PM), https://www.nbcnews.com/nbc-out/out-politics-and-policy/law-professor-khiara-bridges-calls-sen-josh-hawleys-questions-pregnanc-rcna38015 [perma.cc/72F9-YAFR] (although I decided to opt at times to use "women" and the pronoun "she" for conciseness in this Article, I would like to acknowledge that those with the "capacity for pregnancy" can include transgender and non-binary individuals).

[3] *See Abortion Is Central to the History of Reproductive Health Care in America*, PLANNED PARENTHOOD, https://www.plannedparenthoodaction.org/issues/abortion/abortion-central-history-reproductive-health-care-america [perma.cc/865J-9ES8] (last visited Oct. 2, 2023) (providing a brief history of laws regulating access to abortion).

[4] *See* Karl Maier, *The Surveillance State Is a Reality*, BLOOMBERG (June 26, 2020, 6:13 AM), https://www.bloomberg.com/news/newsletters/2020-06-26/the-surveillance-state-is-a-reality [perma.cc/YKR4-L9XX].

[5] *Human Rights Crisis: Abortion in the United States After* Dobbs, HUM. RTS. WATCH (Apr. 18, 2023, 12:01 AM), https://www.hrw.org/news/2023/04/18/human-rights-crisis-abortion-united-states-after-dobbs [perma.cc/M9T8-D4QU].

leave behind as ordinary, technology-reliant members of society.[6] Consequently, law enforcement can conduct vast, invasive sweeps of personal information to mine for evidence of abortion, criminalize women, and, disproportionately, criminalize women of color.[7]

[2] In *Dobbs v. Jackson Women's Health Organization*,[8] the Supreme Court overturned "more than a century's worth of precedent, . . . upended the right to bodily autonomy and privacy for women across the country, and

[6] *Id.*

[7] *See generally* Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 UNIV. BALT. L. REV. 1, 6, 8, 13–14 (2020) (exploring how lack of digital privacy can amplify the criminalization of abortion in minority groups); *see also Hearing on "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security" Before the H. Comm. on Energy and Com. & Subcomm. on Consumer Prot. and Com.*, 117th Cong. 1, 3, 6 (statement of Bertram Lee Jr., Senior Pol'y Couns., Data, Decision Making, and A.I.) (2022), https://docs.house.gov/meetings/IF/IF17/20220614/114880/HHRG-117-IF17-Wstate-LeeB-20220614.pdf [perma.cc/2MML-EL6H] ("[T]he impact of data-intensive technologies on individuals, and marginalized communities in particular, is increasing every day as the pace of innovation accelerates. . . . There is a growing public awareness of how data-driven systems can reflect or reinforce discrimination and bias, even inadvertently."); Juliana Kim, *Data privacy concerns make the post-Roe era uncharted territory*, NPR (July 2, 2022, 3:54 PM), https://www.wesa.fm/2022-07-02/data- privacy-concerns-make-the-post-roe-era-uncharted-territory [perma.cc/8VSM-73PF] ("People of color have always been the guinea pigs for surveillance and for cracking down on any kind of unwanted behavior in the United States."); *see also* Jolynn Dellinger & Stephanie Pell, *The Impotence of the Fourth Amendment in a Post-*Roe *World*, LAWFARE (June 13, 2022, 9:06 AM), https://www.lawfareblog.com/impotence-fourth-amendment-post-roe-world [perma.cc/C74P-Z4E4] (observing that, while some digital security measures exist, these tools "will not be equally accessible to all individuals. Digital literacy, discriminatory surveillance by law enforcement, and poverty will all make privacy and security harder to come by. . . . Minority communities are already subject to a greater degree of suspicion and surveillance, and such discriminatory surveillance will compromise the ability of members of these communities to protect themselves when seeking reproductive health care. Poverty also makes evading surveillance and obtaining services more challenging.").

[8] *See generally* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022).

ignored well-settled law affirming bodily privacy as a fundamental unenumerated right protected by the Constitution."[9] While abortion may continue to be intensely controversial, the idea that the *Dobbs* decision will create long-term socio-economic fallout is not.[10] Enforcement of post-Roe laws will "likely hinge on increased digital surveillance by authorities to more efficiently identify, arrest, and prosecute pregnant people who contemplate or seek abortions."[11]

[3] Rather than resolving the question of abortion's constitutionality, the *Dobbs* decision will render abortion more dominant in the political process than ever, as legislators are motivated to adopt abortion-related laws, whether to protect or ban abortion, and judicial elections focus on state abortion rights.[12] While reproductive health care will continue to be a political hot button, one way to manage some of the fallout from *Dobbs* is by placing over-due limits on state surveillance that protect the politically uncontroversial expectation of privacy for private data. Measures are especially needed to protect the privacy of health care data and, in particular,

[9] Amy Keller & David Straite, Dobbs *Ruling Means It's Time To Rethink Data Collection*, LAW 360 (June 30, 2022, 6:00 PM), https://www.law360.com/articles/1507779/dobbs-ruling-means-its-time-to-rethink-data-collection [perma.cc/93BJ-EJBU].

[10] *See, e.g.*, Erica Kraus & Justine Lei, *Supreme Court Decision in* Dobbs v. Jackson Women's Health Organization *Overturns 50 Years of Precedent on Abortion Laws and Rights*, SHEPPARD MULLIN (July 1, 2022), https://www.sheppardhealthlaw.com/2022/07/articles/provider/supreme-court-decision-dobbs-v-jackson-womens-health-organization-overturns-50-years-of-precedent-on-abortion-laws-rights/ [https://perma.cc/U24X-SGWM] (noting that though perspectives often differ greatly on what the long-term effects of *Dobbs* might be, scholars and journalists on both sides of the aisle have largely agreed that there will be long-term effects).

[11] Cynthia Brumfield, *Data protection concerns spike as states get ready to outlaw abortion*, CSO ONLINE (May 23, 2022), https://www.csoonline.com/article/3661689/data-protection-concerns-spike-as-states-get-ready-to-outlaw-abortion.html [perma.cc/RME7-9PW9].

[12] Erwin Chemerinsky, *Abortion Is About to Dominate American Politics Like Never Before*, TIME (June 27, 2022, 10:43 AM), https://time.com/6191444/abortion-dominate-politics/ [perma.cc/9HCB-7T28].

reproductive health care data. Though there is strong legal footing for the expectation of privacy in one's health care data,[13] law enforcement's largely unencumbered access to that data dramatically illustrates the law's failure to keep pace with technology.

[4] Those who may face prosecution post-*Roe* include practitioners, clinic staff, and even rideshare drivers for mobile apps such as Uber and Lyft, particularly given the number of states that have passed citizen-enforced abortion bans.[14] This Article focuses on the unique vulnerability of women who face prosecution because, by merely using digital devices essential to being a member of society to search, text, or travel for their reproductive care, they have no option but to leave a digital trail that is subject to mining by law enforcement. Anyone seeking reproductive care might leave a digital trail by taking mundane, basic actions, such as "researching reproductive health care online, updating a period-tracking app, or bringing a phone to the doctor's office," any of which have the potential to be used by law enforcement to find and charge those seeking reproductive care.[15] From a normative standpoint, such medical data is

[13] *See The HIPAA Privacy Rule*, U.S. DEPT. HEALTH AND HUM. SERVS. (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html#:~:t…y%20Rule%20establishes,care%20providers%20that%20conduct%20certain [perma.cc/RC58-769A].

[14] *See* Kim, *supra* note 7 (at the time of writing this article, those states included Texas and Idaho); *see also* Jessica Bursztynsky, *Lyft, Uber will cover legal fees for drivers sued under Oklahoma abortion law*, CNBC, https://www.cnbc.com/2022/04/30/lyft-will-cover-legal-fees-for-drivers-sued-under-oklahoma-abortion-law.html [perma.cc/ZL9H-J6GH] (last updated Apr. 30, 2022, 9:40 AM); *see* Oklahoma Call for Reprod. Just. v. State, 202 OK 60 (May 31, 2023), https://reproductiverights.org/wp-content/uploads/2023/05/2023-05-31-Okla-Sup-Ct-Decision-Sb8-Copycats.pdf (illustrating that two Oklahoma state laws banning abortion that included citizen enforcement were overturned in May 2023 by the state supreme court).

[15] Steve Alder, *Bill Seeks to Ban Data Brokers from Selling Health and Location Data*, HIPAA J. (June 17, 2022), https://www.hipaajournal.com/bill-seeks-to-ban-data-brokers-from-selling-health-and-location-data/ [perma.cc/CJC7-R62H] [hereinafter Alder, *Bill Seeks to Ban Data Brokers*] (quoting Sen. Ron Wyden).

deeply personal,[16] with culturally significant[17] reasons existing to protect it and resist "uterus surveillance."[18]

[5] The consequences will be most grave for women of color. According to a report by the U.S. Centers for Disease Control and Prevention, varying abortion rates and ratios have been demonstrated across racial or ethnic groups.[19] In the 2020 study, the CDC found that abortion rates and ratios were 3.9 and 3.6 times higher among black women, and 1.8 and 1.5 times higher among Hispanic women, compared with white women.[20] The CDC noted that "complex" factors lead to the differing reported abortion rates among certain racial or ethnic minority groups, elaborating that[21] "[i]n addition to disparities in rates of unintended pregnancies, structural factors, including unequal access to quality family planning services, economic inequities, and mistrust of the medical system, can contribute to observed differences."[22]

[6] Moreover, disadvantaged women of color are more likely to be targeted, not because of any distinct behavior but simply because they are

[16] *See* Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143, 197 (2017).

[17] *Id*.

[18] Alder, *Bill Seeks to Ban Data Brokers*, *supra* note 15 (quoting Press Release, Sen. Ron Wyden, Wyden, Colleagues Introduce Legislation to Ban Data Brokers from Selling American's Location and Health Data).

[19] Katherine Kortsmit et al., *Abortion Surveillance – United States, 2020*, 71 MMWR SURVEILLANCE SUMMARIES 1, 7 (2022).

[20] *Id.*

[21] *Id.*

[22] *Id.*

more likely to be deemed suspect, often by medical staff.[23] "'Black women who suffered from stillbirths, Black women who had alerted their doctors that they suffered through addiction were being policed, were being stigmatized and ultimately were being arrested . . . [w]hether they had healthy births or whether they had a miscarriage.'"[24] Complicating the issue further, because miscarriages often have no known cause, a self-managed abortion and a miscarriage can be medically indistinguishable.[25] Prosecutors have discretion to "'sweep in anyone who is experiencing a pregnancy loss that they deem 'suspicious'," which tends to be "poor people, people of color, young people . . . ."[26] One prosecutor, at least, has urged heeding lessons learned from the war on drugs.[27] She noted that the failed campaign resulted in law enforcement subjecting persons of color and marginalized communities to "targeted enforcement tactics and disparate sentencing at a greater rate than their white counterparts," which fueled much of the present mass incarceration.[28] Excessive abortion restrictions, she warned, will also lead to the disproportionate criminalization of persons of color and those from vulnerable communities.[29] She has "vowed" not to prosecute those seeking reproductive care, their providers, or those who

[23] Sandhya Dirks, *Criminalization of pregnancy has already been happening to the poor and women of color,* NPR (Aug. 3, 2022, 10:30 AM), https://www.npr.org/2022/08/03/1114181472/criminalization-of-pregnancy-has-already-been-happening-to-the-poor-and-women-of [perma.cc/JD73-ADRA].

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] Sherry Boston, *War On Drugs Is Cautionary Tale For Abortion Prosecution*, LAW 360 (Jan. 20, 2023, 5:06 PM), https://www.law360.com/articles/1567458/war-on-drugs-is-cautionary-tale-for-abortion-prosecution [perma.cc/FQY8-SXV2].

[28] *Id.*

[29] *Id.*

assist them and directly asked other prosecutors to "carefully consider" how they might reduce harm in their own jurisdictions.[30]

[7] Thus, while women will suffer or even die because of physicians' fears of liability for treating pregnancy complications in the face of untested abortion bans,[31] disadvantaged women face the additional threat of criminalization of their pregnancies.[32] "[T]he conversation about pregnancy and abortion is not just about health and physical survival, it's increasingly about prison and policing."[33] For a law enforcement now "being handed even more power to surveil and punish pregnancy and women's bodies,"[34] digital trails generated by ordinary activities can potentially provide evidence to support suspicions[35] that may be "based less on evidence, and more on racism and classism."[36]

[8] As this Article will discuss, the expectation of privacy for health care data finds support in Fourth Amendment jurisprudence and has been

[30] *Id.*

[31] The Political Science Podcast, *Abortion and the Potential "Criminalization of Pregnancy" in the U.S.*, NEW YORKER, at 16.25 (June 29, 2022), https://www.newyorker.com/podcast/politics-and-more/abortion-and-the-potential-criminalization-of-pregnancy-in-the-us [perma.cc/FX7D-PCN2]; *see, e.g.,* Carrie Feibel, *Because of Texas' abortion law, her wanted pregnancy became a medical nightmare*, NPR (July 26, 2022, 5:04 AM), https://www.npr.org/sections/health-shots/2022/07/26/1111280165/because-of-texas-abortion-law-her-wanted-pregnancy-became-a-medical-nightmare [perma.cc/MB59-A8CY].

[32] *See* Dirks, *supra* note 23.

[33] *Id*.

[34] *Id*.

[35] Conti-Cook, *supra* note 7, at 13.

[36] Dirks, *supra* note 23.

protected by federal legislation,[37] but the disconnect between legal protection and digital reality has created unprecedented opportunities for law enforcement. Given the perfect storm of readily accessible troves of private digital information alongside a panoply of inconsistent state solutions,[38] comprehensive federal privacy legislation with dedicated reproductive health care data protections is essential to provide a protective floor.

[9] Part II discusses the historic foundations of the "expectation of privacy" and notes both the limited protection the doctrine provides for digital health care data and that existing federal legislation intended to protect health care data privacy fails to do so.

[10] Part III presents ways law enforcement can obtain health data regarding reproductive choice post-*Roe* without a warrant: first, because of failings in the Health Information Portability and Accountability Act, the federal law created in 1996 to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.[39] Second, law enforcement can obtain reproductive health care data from the ample digital breadcrumbs that fall outside any regulatory construct: either for "free" by subpoenas or orders against data in the cloud or on a server; or by

[37] Ryan Knox, *Fourth Amendment Protections of Health Information After* Carpenter v. United States*: The Devil's In The Database*, 45 AM. J. L. & MED. 331, 340–341, 344–345 (2019); *see* Abigail Sims, *What is Data Privacy in Healthcare? Everything You Need to Know*, TONIC (Aug. 15, 2022), https://www.tonic.ai/blog/what-is-data-privacy-in-healthcare-everything-you-need-to-know [perma.cc/CR6Y-X6Z5].

[38] *See e.g.,* 2020 Cal. Legis. Serv. Prop. 24 (West); VA. CODE ANN. §§ 59.1-575–59.1-585 (West 2023); COLO. REV. STAT. ANN. §§ 6-1-1301–6-1-1313 (West 2023).

[39] *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/phlp/publications/topic/hipaa.html [perma.cc/2FYA-Z972] [hereinafter *HIPPA*] (referencing Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191 (1996)).

purchasing data "for sale" from data brokers.[40] Whether free or for sale, location data is featured prominently, including data obtained via geofence warrants.[41]

[11] Part IV presents the Article's proposal. Federal legislation is needed to provide privacy safeguards not just for digital data generally but for health care data, and specifically health care data relating to reproductive choice. Such legislation must provide "three corners" of data privacy protection. The first corner defines health care data to include a specific carve-out for reproductive health care data. The second corner provides a substantive prohibition against the selling of this reproductive health care data. The third corner furnishes necessary procedural protection: because no other kind of health care data has the broad potential to subject a patient to criminalization, reproductive health care data that would not be obtainable without a warrant should not be admissible as evidence to criminalize the individual.

[12] Part V provides concluding thoughts on repercussions of *Dobbs* beyond reproductive choice. Given the polarized political climate and ascendancy of originalists to the Supreme Court willing to overturn long-

[40] Allan Yeoman et al., *CLOUD Act – Law enforcement access to cloud data*, BUDDLE FINDLAY (May 15, 2018), https://www.buddlefindlay.com/insights/cloud-act-law-enforcement-access-to-cloud-data/ [perma.cc/78GB-X3MA]; *see* Sharon B. Franklin et al., *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, CTR. FOR DEMOCRACY & TECH. (Dec. 9, 2021), https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/ [perma.cc/7CV2-YA6H].

[41] *See, e.g.*, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2509 (2021).

standing precedent,[42] the need to set limits on law enforcement's ability to snoop on private data is more critical than ever.

II. HISTORIC FOUNDATIONS OF "EXPECTATION OF PRIVACY" AND LIMITED VALUE POST-*ROE*[43]

[13] The constitutional right to an expectation of privacy rests on a long history of Fourth Amendment cases.[44] The "right of the people to be secure in their persons, houses, papers, and effects"[45] has been interpreted to mean that a warrant is required to search one's cell phone,[46] obtain cell site location information,[47] affix a tracking device to one's vehicle to monitor its movements on public streets,[48] or aim thermal imaging devices at a person's home.[49] It should also include obtaining an individual's reproductive health care data, which is intensely personal and likewise deserving of protection.[50] The digital era, however, has presented challenges

[42] *See e.g.,* Erwin Chemerinsky, *Op-Ed: How the scourge of originalism is taking over the Supreme Court*, L.A. TIMES (Sept. 6, 2022, 3:15 AM), https://www.latimes.com/opinion/story/2022-09-06/originalism-supreme-court-conservatives-fallacy-robert-bork [perma.cc/U9RQ-PVXP].

[43] *See generally* Eunice Park, *Objects, Places and Cyber-Spaces Post-*Carpenter*: Extending the Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA*, 21 YALE J.L. & TECH. 1, 8–13 (2019) (arguing for extending the third-party doctrine).

[44] *expectation of privacy*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/expectation_of_privacy [perma.cc/FL6Z-KR8Z] (last visited Oct. 2, 2023).

[45] U.S. CONST. amend. IV.

[46] Riley v. California, 573 U.S. 373, 403 (2014).

[47] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[48] United States v. Jones, 565 U.S. 400, 404 (2012).

[49] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[50] *See* Knox, *supra* note 37 at, 346–47; *see also* Terry, *supra* note 16, at 197.

to the Fourth Amendment, with law enforcement invoking the third-party doctrine for data the individual has not voluntarily disclosed in the traditional sense, and in fact, may not even realize was shared with others at all.[51] The following discusses the historical foundations of the expectation of privacy, challenges in applying the Fourth Amendment to digital data, and the need for legislative solutions.

A. Constitutional Origins

[14] The Fourth Amendment's protections mandate that a search or seizure conducted by a government agent must be "reasonable."[52] While there is no right to privacy expressly in the Fourth Amendment, nor any general constitutional right to privacy recognized by the Supreme Court,[53] Fourth Amendment jurisprudence has implicated an expectation of privacy since *Katz v. United States*.[54] The Fourth Amendment originally "was understood to embody a particular concern for government trespass,"[55] but, since *Katz* was decided in 1967, it has also been held to implicate a reasonable expectation of privacy.[56] To invoke Fourth Amendment protection against unreasonable or warrantless searches based on a "*Katz*

[51] Laura Hecht-Felella, *The Fourth Amendment in the Digital Age: How* Carpenter *Can Shape Privacy Protections for New Technologies*, BRENNAN CTR. FOR JUST. N.Y. UNIV. SCH. L., Mar. 18, 2021, at 4–5.

[52] U.S. CONST. amend. IV.

[53] *See* Katz v. United States, 389 U.S. 347, 350 (1967) ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"); *see also* Newhard v. Borders, 649 F. Supp. 2d 440, 449–50 (W.D. Va. 2009) ("[A]ny plausible claim would [not] arise . . . under privacy rights protected by the Constitution[.]") (citing Carroll v. Parks, 755 F.2d 1455, 1457 (11th Cir. 1985)).

[54] *See Katz*, 389 U.S. at 351 ("[T]he Fourth Amendment protects people, not places.").

[55] United States v. Jones, 565 U.S. 400, 406 (2012).

[56] *See id.* at 407–08.

invasion of privacy,"[57] the area searched must be one in which there is a "constitutionally protected reasonable expectation of privacy."[58] The person whose rights were violated must have demonstrated an actual privacy expectation, and that expectation must be one "society is prepared to recognize as 'reasonable.'"[59] In *Katz*, the Court stated that "[o]ne who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[60]

[15] Once a reasonable expectation of privacy has been established, the burden is on the government to justify a warrantless search.[61] Because "the Constitution requires 'that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police[,]'" a warrantless search is per se unreasonable, "subject only to a few specifically established and well-delineated exceptions."[62] Under the exceptions, certain types of searches and seizures are valid even without a showing of probable cause or a warrant.[63] Barring such an exception, an individual's "reasonable

[57] *Id.* at 408 n. 5.

[58] *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

[59] *Id.* at 361.

[60] *Id.* at 352.

[61] *See id.* at 357.

[62] *Id.* (quoting Wong Sun v. United States, 371 U.S. 471, 481–82 (1963)).

[63] *See Katz*, 389 U.S. at 357 n. 19 (citing examples of cases reinforcing the principle that warrantless searches may be valid in exceptional situations, such as searches of items in plain view, brief investigatory stops, and in exigent circumstances).

expectation of privacy" has been considered since *Katz* to be a discrete, measurable expectation, framed in a two-part test.[64]

[16] Subsequent cases determined that an individual forfeits a legitimate expectation of privacy in information he voluntarily turns over to third parties,[65] but the Supreme Court reaffirmed the privacy right in *Riley v. California*[66] by requiring a warrant to search a cell phone.[67] The emphasis on privacy in *Riley* reinforces the *Katz* reasonable expectation of privacy,[68] and in so doing the Court "[took] clear aim at the third-party rule—that 'non-content' records like call logs, location data, and other metadata held by third parties can be collected by the government without a warrant."[69]

[17] This "clear aim"[70] became a direct strike in *Carpenter v. United States*.[71] Although the Government thought it had "clinched the case" by location records that confirmed the defendant was at the site of the robbery

[64] Morgan Cloud, *Property is Privacy: Locke and Brandeis in the Twenty-First Century*, 55 AM. CRIM. L. REV. 37, 42 (2018) (stating that the two-part formula adapted from Justice Harlan's concurrence became the keystone of Fourth Amendment privacy analysis in following years).

[65] United States v. Miller, 425 U.S. 435, 443 (1976); Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[66] *See* Riley v. California, 573 U.S. 373, 373 (2014).

[67] Park, *supra* note 43, at 9–10.

[68] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[69] *See* Marc Rotenberg & Alan Butler, *Symposium: In* Riley v. California*, a unanimous Supreme Court sets out Fourth Amendment for digital age*, SCOTUSBLOG (June 26, 2014, 6:07 PM), http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age [perma.cc/77JZ-PLWB]; *see also* Park, *supra* note 43, at 10.

[70] *See* Rotenberg & Butler, *supra* note 69.

[71] *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

at the time it occurred,[72] the Court held that the Government's acquisition of Carpenter's cell site location information (CSLI) was a Fourth Amendment search requiring a warrant supported by probable cause.[73] The Government had contended that the third-party doctrine governed the case, yet acknowledged the new technology involved.[74] The Court concluded that the Government's "assert[ion] that the legal question nonetheless turns on a garden-variety request for information from a third-party witness . . . fails to contend with the seismic shifts in digital technology" that include "the exhaustive chronicle of location information casually collected by wireless carriers today.[75]

[18] The "intersection of two lines of cases" informed the Court's decision that Carpenter had a privacy interest in his CSLI.[76] The first line involves the expectation of privacy in one's physical location and movements,[77] while the second involves the third-party doctrine's distinction "between what a person keeps to himself and what he shares with others."[78] The Court deemed reliance on the rationale of voluntary exposure unsustainable when it comes to CSLI for two main reasons.[79] First, the

[72] *Id.* at 2213.

[73] *Id.* at 2221.

[74] *Id.* at 2219.

[75] *Id.*

[76] *Carpenter*, 138 S. Ct. at 2214–15.

[77] *Id.* at 2215.

[78] *Id.* at 2215–16.

[79] *Id.* at 2219–20 ("The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another.").

technology is pervasive.[80] Second, information cannot be said to be voluntarily exposed in the absence of an affirmative act.[81] The Court emphasized that "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. . . . [I]n no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements."[82]

[19] Other courts have since echoed the concern that although the rationale behind the third-party doctrine is that Fourth Amendment protections are waived by an individual's voluntary disclosure of information to a third party, "many device users do not voluntarily relinquish information; rather, when the devices are powered on, information is sent on behalf of the individual to third parties. No voluntary action triggers this collection . . . ."[83] The third-party doctrine's premise as an exception to the expectation of privacy loses traction in the digital age.

[20] Through its decision in *Carpenter*, the Court fortified the principle first laid out in *Katz* that the Fourth Amendment protects not only property interests but certain expectations of privacy as well.[84] While acknowledging the tension between property and privacy-based conceptions of the Fourth Amendment, the Court, rather than adhering to an originalist property-based interpretation, looked to history to underscore the Framers' concerns with

[80] *Id.* at 2220 ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society.").

[81] *Carpenter*, 138 S. Ct. at 2220.

[82] *Id.* (citing Smith v. Maryland, 442 U.S. 735, 745 (1979)).

[83] *See, e.g.*, *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 737 (N.D. Ill. 2020) (quoting Cristina Del Rosso & Carol M. Bast, *Protecting Online Privacy in the Digital Age*: Carpenter v. United States *and the Fourth Amendment's Third-Party Doctrine,* 28 CATH. UNIV. J.L & TECH. 89, 120–21 (2020)).

[84] *Carpenter*, 138 S. Ct. at 2213 (citing Katz v. United States, 389 U.S. 347, 351 (1967)).

government intrusion.[85] It saw the Fourth Amendment as aiming to "secure the 'privacies of life' against 'arbitrary power[,]'" and "'place obstacles in the way of a too permeating police surveillance.'"[86] The Court found itself "obligated . . . to ensure that the 'progress of science' does not erode Fourth Amendment protections,"[87] and even declared that in cases involving "innovations in surveillance tools," the Fourth Amendment "'assure[s] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[88]

B. Digital Data Challenges and Limited Protections

1. Doctrinal Dilemmas, Possible Solutions

[21] *Carpenter* thus anticipated that the "progress of science" and "innovations in surveillance tools" will continue to pose challenges to historic privacy protections.[89] One way to maintain the third-party doctrine's viability is to take a subtler look at the concept of voluntariness.[90] An expectation of privacy—subjective and objective, under the *Katz* test—should not be forfeited simply because a third party owns or controls an

[85] *Id.*

[86] *Id.* at 2214 (citations omitted).

[87] *Id.* at 2223 (citing Olmstead v. United States, 277 U.S. 438, 473–474 (1928) (Brandeis, J., dissenting)).

[88] *Id.* at 2214 (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)); *see generally* Barry Friedman, *Private Data/Public Regulation* (N.Y.U. Sch. of L, Working Paper No. 22-35, 2022).

[89] *Carpenter*, 138 S. Ct. at 2209, 2223 (citations omitted).

[90] *See* Park, *supra* note 43, at 10, 13–17 (suggesting that a retrospective two-part test can be applied as an extension of the third-party doctrine in the absence of an affirmative act of sharing digital data).

individual's personal data, as the *Carpenter* dissent would have it.[91] Nor should an expectation of privacy be assumed simply because the data is automatically shared with a third party. Rather, when there is no affirmative act of sharing, the third-party doctrine test could be a more nuanced, retrospective one, involving two inquiries: first, whether the individual understood that the technology necessitated sharing data with a third party; and second, whether the individual had a meaningful opportunity to opt out of that sharing,[92] or even better, opt in.[93] Allowing for the possibility that limited circumstances may arise in which the government can legitimately pass the two-part retrospective test aligns with the American ethos of individuality[94] that the third-party doctrine reflects, by preserving room for the opportunity to make a choice. Barring that, however, a warrantless

[91] *See Carpenter*, 138 S. Ct. at 2223–35 ("This case should be resolved by interpreting accepted property principles as the baseline for reasonable expectations of privacy. Here the Government did not search anything over which Carpenter could assert ownership or control. Instead, it issued a court-authorized subpoena to a third party to disclose information it alone owned and controlled. That should suffice to resolve this case.") (Kennedy, J., dissenting, joined by Thomas, J., Alito, J.).

[92] Park, *supra* note 43, at 14.

[93] *See* Letter from India McKinney, Dir. of Fed. Affs., Elec. Frontier Found., to Frank Pallone Jr., Chair, House Comm. on Energy & Com, Janice D. Schakowsky, Chair, Subcomm. on Consumer Prot. and Com., House Comm. on Energy & Com., Cathy McMorris Rodgers, Ranking Member, House Comm. on Energy & Comm., & Gus M. Bilirakis, Ranking Member, Subcomm. on Consumer Prot. and Com., House Comm. on Energy & Com. (June 13, 2022), https://www.eff.org/files/2022/06/14/2022.06.13_eff_letter_to_house_enc_re._hearing_on_protecting_americas_consumers_.pdf [perma.cc/2B2N-8KVA].

[94] Colloquial phrases such as "pulling oneself up by one's bootstraps" and "rugged individualism" reflect the high importance the American culture places on the individual. For a general discussion of American individualism, *see, e.g.*, Ava Rosenbaum, *Personal Space and American Individualism*, BROWN POLITICAL REVIEW (Oct. 31, 2018), https://brownpoliticalreview.org/2018/10/personal-space-american-individualism/ [https://perma.cc/HCV4-HNHU] ("The United States has one of the most individualistic cultures in the world. Americans are more likely to prioritize themselves over a group and they value independence and autonomy. This societal ethos can be seen in how Americans relate to each other…").

search of digital data conducted under the authority of the third-party doctrine should be unconstitutional.[95]

[22] In the meantime, at least one pair of scholars has urged that *Carpenter* outright replace *Katz* as the primary test in Fourth Amendment law.[96] The *Carpenter* "multifactor test will lead to more predictability" and "resonates more directly with the Fourth Amendment's history," in that "[i]t treats the Fourth Amendment as a restriction on the government's power to obtain information on its citizens, and not solely as a protector of privacy."[97] Replacing *Katz* with the *Carpenter* test would "impel[] courts to engage in a deep consideration of the specific features of technology and society's embrace of technology that was usually lacking from the conventional *Katz* test."[98] Doing so would also be consistent with the European Union's data protection regime rather than the traditional U.S. consumer-focused consent framework of data privacy, a shift this Article supports in Part IV.[99]

[23] Moreover, the Fourth Amendment provides no protection where a warrant is not necessary.[100] The digital era has allowed "[w]hat was once a practice of targeted data collection [to] . . . tur[n] into bulk data gathering"

---

[95] *See* In re Search of Info. Stored at Premises Controlled by Google, 481 F.Supp.3d 730, 737 (ND. Ill. 2020) (quoting Cristina del Rosso & Carol M. Bast, *Protecting Online Privacy in the Digital Age:* Carpenter v. United States *and the Fourth Amendment's Third-Party Doctrine*, 28 CATH. UNIV. J. L. & TECH. 89, 120–21 (2020)).

[96] *See* Matthew Tokson & Paul Ohm, *Carpenter Should Replace* Katz *in Fourth Amendment Law*, LAWFARE (July 13, 2022, 8:01 AM), https://www.lawfareblog.com/carpenter-should-replace-katz-fourth-amendment-law# [perma/cc/MNS3-ZNRG].

[97] *Id.*

[98] *Id.*

[99] *See infra* Part IV.

[100] *See What Does the Fourth Amendment Mean?*, U.S. CTS, https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0 [perma.cc/XQR2-ZXWE] (last visited Oct. 16, 2023).

via "GPS and cell-site location information, biometric databases, license plate locations, and more."[101] Such surveillance data eludes the Fourth Amendment's warrant requirement, because collecting such data, or purchasing it on the private market,[102] is not even considered a search under the Fourth Amendment.[103]

2. Political Pitfalls, Limited Legislation

[24] Not only does the Fourth Amendment face limits outside the analog world of footlockers and physical containers,[104] but the legitimacy of the Supreme Court as the third branch in the federal system of checks and balances has been eroding.[105] To rely on the Supreme Court to interpret and apply Fourth Amendment precedent is to assume that the body is non-political and non-partisan and views its role as limited to interpreting and applying precedent—within a range of potential legal philosophies, but

[101] Farhang Heydari, *Understanding Police Reliance on Private Data* (Hoover Inst., Aegis Series Paper No. 2106, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4095489 [perma.cc/47DS-4W8J].

[102] *See* Friedman, *supra* note 88, at 3.

[103] *Id.* at 16.

[104] *See* United States v. Chadwick, 433 U.S. 1, 11 (1977) ("By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination[.]"); *see also* New York v. Belton, 453 U.S. 454, 461 (1981) (stating that any container, "whether it is open or closed," in the car's passenger compartment may be searched, since a "lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have.").

[105] Zack Beauchamp, *What happens when the public loses faith in the Supreme Court?*, Vox, https://www.vox.com/23055620/supreme-court-legitimacy-crisis-abortion-roe [perma.cc/3M2M-W6F2] (last updated June 26, 2022, 11:01 AM).

independent of personal agendas.[106] However, with "militant conservatism now triumphant at the high court,"[107] and ethics concerns growing with revelations that Supreme Court Justices Thomas and Alito accepted luxurious gifts without disclosing them,[108] such a balance cannot be assumed.

[25] Without term limits for Supreme Court appointees, it will be the legislative branch, with cyclical elections, where the members will represent most constituents' viewpoints most of the time.[109] The decision in

---

[106] *See* Morning Edition, *Is the Supreme Court majority ruling on the law or their personal preference?*, NPR, at 00:26 (July 19, 2022, 5:06 AM), https://www.npr.org/2022/07/19/1112219517/is-the-supreme-court-majority-ruling-on-the-law-or-their-personal-preference [perma.cc/B85N-L4BR].

[107] Jacob Heilbrunn, *He Was Dismissed as a Conservative Kook. Now the Supreme Court Is Embracing His Blueprint*, POLITICO (July 7, 2022, 4:30 AM), https://www.politico.com/news/magazine/2022/07/07/leo-brent-bozell-abortion-game-00044246 [perma.cc/4JAQ-6TDW].

[108] Li Zhou, *The Supreme Court has an ethics problem. Justice Alito's fishing trip is the latest proof.*, VOX (June 21, 2023, 2:30 PM), https://www.vox.com/scotus/2023/6/21/23768710/supreme-court-samuel-alito-luxury-fishing-trip-propublica-wsj-ethics-problem [perma.cc/NE6J-HBGU]; Ian Millhiser, *The Supreme Court's tone-deaf response to the Clarence Thomas corruption scandal*, VOX (Apr. 26, 2023, 2:05 PM), https://www.vox.com/politics/2023/4/26/23698962/supreme-court-clarence-thomas-corruption-ethics-harlan-crown-john-roberts-dick-durbin [https://perma.cc/NJ8P-M7H8].

[109] *Compare* Sean Illing, *How to save democracy from the Supreme Court*, VOX (Aug. 5, 2022, 6:00 AM), https://www.vox.com/23055652/vox-conversations-supreme-court-democracy-abortion-rights-niko-bowie [https://perma.cc/B579-DS5L] (quoting Niko Bowie: "[W]e have these fundamental disagreements about . . . guns . . . , abortions . . . , and [the] impending climate catastrophe[.] Which institutions should be responsible for resolving these fundamental disagreements? [I]t's no answer to say, well, whatever the Constitution says. . . . In most other democratic societies, national legislatures are responsible for making these determinations, particularly democratically responsive national legislatures."); *with* Tom McCarthy & Alvin Chang, '*The Senate is broken': system empowers white conservatives, threatening US democracy*, THE GUARDIAN (Mar. 12, 2021, 10:00 PM), https://www.theguardian.com/us-news/2021/mar/12/us-senate-system-white-conservative-minority [perma.cc/4Y7T-X43N].

Dobbs starkly illustrates the need for legislative action because it not only undermined the right of reproductive choice, but also the constitutional underpinnings of other rights developed by the Court since *Katz*.[110] In his concurrence, Justice Thomas argued that "the purported right to abortion is not a form of 'liberty' protected by the Due Process Clause" as stated in *Roe*.[111] Thomas stated that the Court had instead "divined a right to abortion" and deemed its "preferred manifestation of 'liberty'" to be "'broad enough to encompass a woman's decision whether or not to terminate her pregnancy.'"[112] He also expressly invited challenges to other long-standing precedent that established hard-gained freedoms in his *Dobbs* concurrence.[113] To protect the privacy of health care data relating to

[110] *See* Larissa Jimenez, *60 Days After Dobbs: State Legal Developments on Abortion*, BRENNAN CTR. FOR JUST. (Aug. 24, 2022), https://www.brennancenter.org/our-work/research-reports/60-days-after-dobbs-state-legal-developments-abortion [perma.cc/K247-Q8LG].

[111] Dobbs v. Jackson Women's Health Org., 142 S.Ct. 2228, 2300 (2022) (Thomas, J., concurring).

[112] *Id*. at 2302 (quoting Roe v. Wade, 410 U.S. 113, 153 (1973) and Planned Parenthood of Southeastern Pa. v. Casey, 505 U.S. 833, 930 (1992)).

[113] *Dobbs,* 142 S.Ct. at 2301 (Thomas J., concurring) ("[I]n future cases, we should reconsider all of this Court's substantive due process precedents, including *Griswold*, *Lawrence*, and *Obergefell*."); *see also* The Associated Press, *Alabama is using the case that ended Roe to argue it can ban gender-affirming care*, NPR (July 3, 2022, 11:03 AM), https://www.npr.org/2022/07/03/1109613520/alabama-abortion-rights-gender-affirming-care-law [perma.cc/X772-LMTH] (noting that already, Alabama has asked a federal appeals court "to lift an injunction and let it enforce an Alabama law that would make it a felony to give puberty blockers or hormones to transgender minors to help affirm their gender identity."); *see, e.g.*, Shira Stein, *Hospital Chain Blocks Fertility Coverage for Its LGBTQ Employees*, BLOOMBERG L., https://www.bloomberglaw.com/bloomberglawnews/health-law-and-business/XCPDIBCC000000?bna_news_filter=health-law-and-business#jcite [perma.cc/RK6S-62SM] ("An Illinois-based Catholic hospital system that employs more than 24,000 people will only cover fertility treatment for workers in opposite-sex marriages . . . . By limiting benefits to opposite-sex spouses, the OSF policy reflects one of the first instances of an employer explicitly excluding workers from coverage not because of objections to the treatment they are seeking but because of their sexual orientation . . . .") (last updated July 18, 2022, 2:59 PM).

reproductive choice and maintain other constitutional protections that Thomas questions, including contraception, legislative solutions must be sought, from democratically accountable representatives.

[26] Although existing federal legislation has already carved out specific protections for health care data, their effectiveness is limited.[114] The express purpose of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was to create "national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[115] HIPAA was followed by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). HITECH "encouraged healthcare providers to adopt electronic health records and improve privacy and security protections for healthcare data," and "strengthened existing HIPAA standards and mandated breach notifications."[116] While HITECH did "expand[] direct applicability and enforcement to business associates," it did not expand privacy rules to "deal with health-care data existing outside of the HIPAA-zone."[117]

[27] Other legislative efforts include the Federal Food, Drug, and Cosmetic Act (FD&C),[118] "which regulates the safety and effectiveness of

[114] Press Release, The White House, Fact Sheet: Biden-Harris Administration Announces Actions to Protect Patient Privacy at the Third Meeting of the Task Force on Reproductive Healthcare Access (Apr. 12, 2023).

[115] *HIPAA*, *supra* note 39.

[116] Steve Alder, *What is the HITECH Act?*, HIPAA J., https://www.hipaajournal.com/what-is-the-hitech-act/ [perma.cc/TM3L-ZQZN] [hereinafter Alder, *What is the HITECH Act?*] (last visited Oct. 9, 2023).

[117] Terry, *supra* note 16, at 164.

[118] 21 U.S.C. §§ 301–360.

medical devices."[119] The Food and Drug Administration's (FDA) role in enforcing the FD&C for mobile medical apps, however, focuses only on "a small subset . . . that may affect the performance or functionality of regulated medical devices, or may pose a higher risk to patients if they do not work as intended."[120] The FDA issued its "Guidance for Industry and Food and Drug Administration Staff" to "clarify the subset of software functions to which FDA intends to apply its authority,"[121] but even so provides a limited definition of a mobile application that will be considered a medical mobile application: it must incorporate device software functionality that meets the definition of device in the FD&C and must be intended either to be used as an accessory to a regulated medical device, or to transform a mobile platform into a regulated medical device.[122] Moreover, the effort at incorporating mobile medical apps is only a recommendation, not a regulation resulting from formal rulemaking, and the Guidance's recommendations are nonbinding.[123]

[28] The Federal Trade Commission Act also provides opportunities for the Federal Trade Commission (FTC) to reach mobile medical apps through Section 45(a), which forbids unfair business practices.[124] The FTC's

[119] Chad Ehrenkranz et al., *Digital Health Cos. Should Expect More Scrutiny Amid Growth*, LAW360 (Aug. 16, 2022, 6:44 PM), https://www.law360.com/articles/1521440/digital-health-cos-should-expect-more-scrutiny-amid-growth [perma.cc/2XEW-ADN8].

[120] *Id*.

[121] U.S. FOOD & DRUG ADMIN., POLICY FOR DEVICE SOFTWARE FUNCTIONS & MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY & FOOD & DRUG ADMINISTRATION STAFF 1 (2022).

[122] *Id.* at 5.

[123] *Id.* at 1.

[124] Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (prohibiting "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.").

allegations against Flo Health Inc., the developer, operator and seller of the Flo Period and Ovulation Tracker app ("Flo"),[125] reflects the FTC's willingness to pursue such app developers and the data they collect that largely falls outside HIPAA's protections.[126] In a press release on the FTC's 2021 settlement with Flo Health Inc., Andrew Smith, Director of the Commission's Bureau of Consumer Protection, stated, "Apps that collect, use, and share sensitive health information can provide valuable services, but consumers need to be able to trust these apps . . . . We are looking closely at whether developers of health apps are keeping their promises and handling sensitive health information responsibly."[127]

[29] HIPAA, however, remains the primary legislation addressing the use and disclosure of individuals' health information. The following section discusses ways law enforcement can circumvent intended protections and obtain private reproductive health care data by capitalizing on exceptions and gaps in HIPAA's statutory language; and by casting wide, unindividualized nets that evade the Fourth Amendment, including by purchasing data in the private market.

III. REPRODUCTIVE HEALTH CARE DATA: WAYS LAW ENFORCEMENT CAN OBTAIN DATA WITHOUT A WARRANT

[30] Law enforcement can access reproductive health care data without a warrant via well-known gaps in HIPAA's outdated regulatory

[125] *See infra* Part III.B.2.b.

[126] Ehrenkranz et al., *supra* note 119.

[127] Press Release, Fed. Trade Comm'n, Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data (Jan. 13, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about [perma.cc/BJ5H-CWJ8].

framework[128] and statutory exceptions that can be taken advantage of post-*Roe* despite their purpose. Moreover, these exceptions and gaps coexist alongside an even more vast array of digital breadcrumbs from which law enforcement can obtain reproductive health care data. Those breadcrumbs reside essentially for free in the cloud or on servers,[129] or can be purchased from data brokers.

A. Regulatory Failings: HIPAA Post-*Roe*

1. Exceptions: Privacy Rule Permissible Disclosures

[31] Despite its purpose, HIPAA provides little, if any, privacy protection against law enforcement seeking reproductive health care data without the individual's consent.[130] Although HIPAA was intended to protect sensitive patient health information by prescribing rules for use and disclosure under its "Privacy Rule,"[131] protected health information ("PHI"),[132] even within HIPAA's auspices, can be disclosed under certain exceptions,[133] and law

[128] *See, e.g.*, Alexis Guadarrama, Comment, *Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry*, 55 HOUS. L. REV. 999, 1010 (2018); Terry, *supra* note 16, at 181–82.

[129] *See* Paul Diamond, *Cloud storage vs. on-premises servers: 9 things to keep in mind*, MICROSOFT (Sept. 25, 2020), https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers (explaining that cloud storage is virtual storage provided by an outside service provider, in contrast to traditional, on-site storage on physical local servers).

[130] *See* Eric Boodman et al., *HIPAA won't protect you if prosecutors want your reproductive health records*, STAT (June 24, 2022), https://www.statnews.com/2022/06/24/hipaa-wont-protect-you-if-prosecutors-want-your-reproductive-health-records/ [perma.cc/J9N4-BUXB].

[131] *HIPAA*, *supra* note 39.

[132] 45 C.F.R. § 160.103 (2013) (defining "protected health information).

[133] *See HIPAA*, *supra* note 39.

enforcement may opt to seize upon some of the loopholes in the language to obtain health records from covered entities and their business associates.

[32] Post-*Dobbs* guidance from the Department of Health and Human Services (HHS) anticipates a need to guard reproductive health care records from law enforcement.[134] In an effort to support access to "comprehensive reproductive health care services, including abortion care, [which] is essential to individual health and well-being," the HHS issued a guidance document entitled "HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care" that addresses the extent to which the Privacy Rule permits use or disclosure of an individual's information regarding "abortion and other sexual and reproductive health care" without the individual's authorization.[135] The guidelines reinforce that entities regulated under HIPAA[136] can use or disclose PHI "*only* as expressly permitted or required by the Privacy Rule," and that disclosures are "narrowly tailored to protect the individual's privacy and support their access to health services."[137] However, despite the HHS' strongly-worded warning, the language of the exceptions leaves room for interpretation. The HHS' position that a regulated entity is never required by HIPAA to disclose PHI appears to rely on a semantic emphasis of the word "required," creating space for non-required, but still permissible, disclosures.

[33] The exceptions that the HHS addresses in the guidelines that permit PHI disclosures relating to health care, "including information relating to

[134] Off. for Civ. Rts., *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, U.S. DEP'T HEALTH & HUM. SERVS. (June 29, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html [perma.cc/3Z9K-YQXF].

[135] *Id.*

[136] *Id.*

[137] *Id*. (emphasis removed) (citing 45 C.F.R. §164.502 (2022)).

abortion and other sexual and reproductive health care,"[138] highlight this weak link. The three permissions for disclosing PHI without an individual's authorization are disclosures required by law; disclosures for law enforcement purposes; and disclosures to avert a serious threat to health or safety.[139] Despite the HHS' interpretation of HIPAA to protect reproductive health care data across these three exceptions, ambiguity in the HHS guidelines with an emphasis on what is "required" versus "permitted" creates opportunities for actors to request and for covered entities to disclose such sensitive data.

a. Disclosures Required by Law

[34] According to the guidelines themselves, "[t]he Privacy Rule permits but does not require covered entities to disclose PHI about an individual, without the individual's authorization, when such disclosure is required by another law and the disclosure complies with the requirements of the other law."[140] An example of a "disclosure required by another law" could be a state requirement to report abortion. Although the HHS emphasizes that the Privacy Rule does not "require" covered entities to disclose PHI about an individual without the individual's authorization, the rule provides that a covered entity "may" disclose protected health information without authorization if the disclosure is within limitations.[141]

[35] The HHS provides the example of an individual who visits a hospital emergency department for complications related to a miscarriage during the tenth week of pregnancy, whom a hospital employee suspects may have

[138] *Id.*; *see* 45 C.F.R. § 164.512(f) (2022).

[139] Off. for Civ. Rts., *supra* note 134.

[140] *Id.* (citing 45 C.F.R. § 164.502) (emphasis removed).

[141] 45 C.F.R. § 164.512(a)(1) (2022) ("A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.").

taken medication to end the pregnancy.[142] According to the HHS, the Privacy Rule would not permit the workforce member to disclose PHI to law enforcement under the "required by law" exception where the state law "does not expressly require such reporting."[143] Despite the boldface emphasis that "the Privacy Rule "would not permit a disclosure to law enforcement under the 'required by law' arm of the exception,"[144] the language may leave room for a disclosure under the "permissible" arm, allowing a review board or court to determine that although not required to disclose PHI, a covered entity can still choose to do so pursuant to a court-ordered warrant, subpoena, or summons.

b. Disclosures for Law Enforcement Purposes

[36] Similarly, the HHS emphasizes that under the Privacy Rule, a request for abortion records for example, accompanied by a court order or warrant,[145] permits but "does not require" a covered entity to disclose PHI about an individual.[146] The HHS takes the opportunity to further qualify that the entity can disclose only the requested PHI if all the conditions the Privacy Rule specifies are met.[147]

[37] The HHS can easily make a case for protection where law enforcement presents no court or other order. "In the absence of a mandate enforceable in a court of law," a staff member of a health care provider may neither initiate nor respond to a law enforcement request to make such a

[142] Off. for Civ. Rts., *supra* note 134.

[143] *Id.* (emphasis removed).

[144] *Id.* (emphasis removed).

[145] *Id.* (emphasis in original) (citing 45 C.F.R. § 164.512(f)(1)).

[146] *Id.* (emphasis removed).

[147] Off. for Civ. Rts., *supra* note 134.

disclosure, because, simply, no reporting requirement exists.[148] Nor do state laws require health care providers generally to report an individual's self-managed pregnancy loss to law enforcement.[149] The purpose of state fetal homicide laws, similarly, is to protect, not penalize, the pregnant individual.[150] Indeed, "'appellate courts have overwhelmingly rejected efforts to use existing criminal and civil laws intended for other purposes (*e.g.,* to protect children) as the basis for arresting, detaining, or forcing interventions on pregnant' individuals."[151] The HHS likewise observes that the Privacy Rule permission relating to reports of child abuse or neglect would not apply to disclosures of PHI relating to reproductive health care.[152] However, all of these examples to buttress patient privacy center on the HHS' reliance on the absence of a requirement to disclose. The absence of a requirement does not refute the possibility of a disclosure that is permissible.

c. Disclosures to Avert a Serious Threat to Health or Safety

[38] Under the third and final exception, the HHS guideline again hinges on the discretionary nature of the regulatory exception. The HHS provides the limitation, carefully stated, that the Privacy Rule "permits but does not require" a covered entity to disclose PHI if the covered entity believes disclosure is necessary to avert a "serious and imminent threat" to health or

[148] *Id.*

[149] *Id.*

[150] *Id.*

[151] *Id.* (quoting 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 POLS., POL'Y & L. 299, 322 (2013)).

[152] Off. for Civ. Rts., *supra* note 134 (citing 45 C.F.R. § 164.512(b)(1)(ii)).

safety.[153] The HHS explicitly states that statements relating to the "intent to get a legal abortion," or to pregnancy or pregnancy complications do not qualify as such a threat.[154] Indeed, such a disclosure "generally would be inconsistent with professional ethical standards . . . ."[155] However, a state that classifies an abortion as a homicide[156] may disagree with the HHS' interpretation. Such a state may instead assert that law enforcement's request for information such as the date and time of treatment[157] is indeed for a permitted disclosure because it is "for the purpose of identifying or locating a suspect . . . or material witness"[158] to the patient's own abortion. Going forward, states may attempt to use this part of HHS' guidance and legislate that a doctor must "report an individual who self-managed the loss

[153] *Id.* (emphasis removed) (citing American College of Obstetricians and Gynecologists) (American Medical Association (citations omitted)).

[154] *Id.*

[155] *Id.*

[156] *See* Elizabeth Dias, *Inside the Extreme Effort to Punish Women for Abortion*, N.Y. TIMES (July 1, 2022), https://www.nytimes.com/2022/07/01/us/abortion-abolitionists.html?referringSource=articleShare [https://perma.cc/KP97-LCX5] (explaining among the antiabortion activists is an extreme group "pursu[ing] what they call 'abortion abolition,' a move to criminalize abortion from conception as homicide, and hold women who have the procedure responsible—a position that in some states could make those women eligible for the death penalty." The group "pushed a bill in Louisiana that would have classified abortion as homicide and enabled prosecutors to bring criminal cases against women who end a pregnancy. The measure failed, but it got further than any of the other 'equal protection' bills abolitionists have worked to introduce in about a dozen states over the past two years.").

[157] 45 C.F.R. § 164.512(f)(2)(i)(F) (2016).

[158] 45 C.F.R. § 164.512(f)(2).

of a pregnancy to law enforcement,"[159] enabling law enforcement to assert that a disclosure for such purposes is, in fact, required.

[39] Finally, under Disclosures Required by Law, the regulatory language creates a great deal of discretion by providing that the "disclosure is limited to the relevant requirements of such law"[160] without defining what that means. The ambiguity provides latitude both for law enforcement to decide what information it needs and for a records custodian, nervous in the uncertain post-*Dobbs* environment, to decide what information to provide. The limitation is unlikely to provide a meaningful guard rail on what reproductive health care records will remain private upon law enforcement request. However, the most important weakness in the exceptions remains the language that centers around what is not required, versus what is actually prohibited.

2. Gaps: "Covered Entities" as Records Custodians

[40] Not only do the exceptions create opportunities to pierce privacy protections of patients post-*Roe*, but HIPAA profoundly exemplifies the law's failure to keep pace with technology by expecting only "covered entities" to be the custodians of health care records.[161] Patient health records

[159] Off. for Civ. Rts., *supra* note 134 (citing *Abortion Access: Know Your Rights*, IF/WHEN/HOW (2023), https://www.reprolegalhelpline.org/know-your-rights/ [https://perma.cc/7WCA-NV5B]).

[160] *See id.; see also* Karen N. Brown, *Allowable HIPAA Exceptions in Emergency Situations*, GE HEALTH (Apr. 8, 2019), https://www.volusonclub.net/empowered-womens-health/allowable-hipaa-exceptions-in-emergency-situations/ [https://perma.cc/G463-HFCV] ("[T]he information released must always be the 'minimum necessary,' except for treatment purposes, and must use reasonable means to keep the patient's information protected from unauthorized use.").

[161] Off. for Civ. Rts., *supra* note 134 (providing, "The Office for Civil Rights (OCR) administers and enforces the Privacy Rule, which establishes requirements with respect to the use, disclosure, and protection of PHI by covered entities (health plans, health care clearinghouses, and most health care providers) and, to some extent, by their business associates.").

are no longer physical charts tucked into manila folders alphabetically filed in a doctor's office. Health records now may be generated digitally by "healthtech," or digital health care technology.[162] Examples include mobile applications, or "apps," which can be created by consumer-facing companies such as Apple and Facebook[163] and include wearable devices like smart watches or fitness trackers; or by remote monitoring by a care provider with health Internet of Things (IoT) devices.[164] However, since HIPAA's privacy rules only address the use and disclosure of individuals' health information by "covered entities," only data collected, used, or maintained by covered entities is subject to HIPAA's privacy rule.[165] This is true even though this same data would be protected had it been provided to a covered entity.[166] As another author has summarized: "Simply put, the

[162] *See* Daniel Cohen et al., *Healthtech in the fast lane: What is fueling investor excitement?*, MCKINSEY & CO. (Dec. 1, 2020), https://www.mckinsey.com/industries/life-sciences/our-insights/healthtech-in-the-fast-lane-what-is-fueling-investor-excitement [https://perma.cc/8QY2-CHWH] (describing growing markets within healthtech).

[163] *See* Katherine Bindley, *Your Health Data Isn't as Safe as You Think*, WALL ST. J., https://www.wsj.com/articles/your-health-data-isnt-as-safe-as-you-think-11574418606 [https://perma.cc/LKK4-5QMJ] (last updated Nov. 22, 2019, 1:15 PM).

[164] *See* Tawanna Lee & Antonio Reynolds, *All Data Is Not HIPAA Data – Healthcare Covered Entities Should Pay Close Attention to State Privacy Laws Regulating the Health IoT Ecosystem*, JD SUPRA (July 13, 2021), https://www.jdsupra.com/legalnews/all-data-is-not-hipaa-data-healthcare-3523068/ [https://perma.cc/9RJD-92E3]; *see also* Ryan Mueller, Note, *Big Data, Big Gap: Working Towards a HIPAA Framework that Covers Big Data*, 97 IND. L. J. 1505, 1511–16 (2022).

[165] *See Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CTRS. FOR DISEASE CONTROL & PREVENTION (June 27, 2022), https://www.cdc.gov/phlp/publications/topic/hipaa.html#print [https://perma.cc/XFW6-EQXS]; *see also Health App Use Scenarios & HIPPA*, DEP'T HEALTH & HUMAN SERVS. (Feb. 2016), https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf; *see also* Mueller, *supra* note 164, at 1507–11.

[166] Lee & Reynolds, *supra* note 164.

amount of protection health data receives depends on who holds the data, not the type of information being held."[167]

[41] Even at a classic covered entity like a hospital, tracking tools installed on websites can collect sensitive information, such as "details about their medical conditions, prescriptions, and doctor's appointments," that is sent to Facebook.[168] At least some hospitals have responded to the findings that patient information was being sent to Facebook by removing the trackers from their websites or patient portals.[169]

[42] Meanwhile, outside the formal covered entity architecture, healthtech generates vast amounts of data.[170] Individuals interacting with mobile health systems generally do so not as a patient but as a consumer, independent of any formal health care provider.[171] The information

[167] Guadarrama, *supra* note 128, at 999; *see also* Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy*, 95 NOTRE DAME L. REV. 155, 158–59 (2019); *see also* Justin Evans & Katelyn Ringrose, *From Fitbits to Pacemakers: Protecting Consumer Privacy and Security in the Healthtech Age*, 68 CLEV. ST. L. REV. 1, 8–9 (2019).

[168] Patrick Malone & Assocs., *Hidden code leaks private data from hospitals and 'pregnancy centers'*, JD SUPRA (July 5, 2022), https://www.jdsupra.com/legalnews/hidden-code-leaks-private-data-from-1988838/ [https://perma.cc/7CNA-5Z9B] (quoting Stat, a health, science, and medicine site, and the tech-focused The Markup news organization, who reported that "[a] tracking tool installed on many hospitals' websites has been collecting patients' sensitive health information . . . and sending [them] to Facebook."); Nicole Wetsman, *Hospital websites are sending medical information to Facebook*, VERGE (June 16, 2022, 10:48 AM), https://www.theverge.com/2022/6/16/23170886/hospital-websites-meta-pixel-tracker-facebook-hipaa [https://perma.cc/DEA2-BSFD] (reporting on the same findings from The Markup that "hospital websites have a tracking tool that sends sensitive medical information to Facebook when [patients] schedule appointments").

[169] Wetsman, *supra* note 168.

[170] *See* Lee & Reynolds, *supra* note 164.

[171] Terry, *supra* note 16, at 181.

generated is sold to third parties in the health information ecosystem that falls entirely outside HIPAA's purview,[172] because the privacy rules did not anticipate that commercial entities seeking an audience for targeted advertising would become the custodians of health records by collecting and generating huge amounts of data.[173] As a result, "consumers are left at the mercy of the device's or app's privacy policy, which can change over time and may allow downstream disclosure and use of sensitive health data."[174]

[43] The HHS issued a proposed rule for changes to HIPAA in December 2020,[175] with a Final Rule expected to be issued in 2023.[176] While defining a Personal Health Application as "an application used by an individual to

[172] Boodman et al., *supra* note 130 (explaining HIPAA does not provide protection of medical data transmitted outside of a medical setting, where third parties disclose health information transmitted via social media sites, online shopping accounts, text messages, for example).

[173] Bindley, *supra* note 163 (identifying the risk of negative consequences for patients who might see targeted ads related to their health conditions due to breach of privacy).

[174] Lee & Reynolds, s*upra* note 164.

[175] Press Release, U.S. Dep't Health & Hum. Servs., HHS Proposes Modification to the HIPAA Privacy Rule to Empower Patients, Improve Coordinated Care, and Reduce Regulatory Burdens (Dec. 10, 2020), https://public3.pagefreezer.com/content/HHS.gov/31-12-2020T08:51/https:/www.hhs.gov/about/news/2020/12/10/hhs-proposes-modifications-hipaa-privacy-rule-empower-patients-improve-coordinated-care-reduce-regulatory-burdens.html [https://perma.cc/N6HS-6ZL6].

[176] *See* Steve Alder, *New HIPAA Regulations in 2023*, HIPAA J. (May 1, 2023), https://www.hipaajournal.com/new-hipaa-regulations/ [https://perma.cc/2DV3-QZRX] [hereinafter Alder, *New HIPAA Regulations in 2023*]; *see also* Carol Amick, *Are HIPAA Changes Coming?*, COMPLIANCEPOINT (June 13, 2022), https://www.compliancepoint.com/healthcare/coming-changes-to-hipaa/ [https://perma.cc/J96F-LEES] (predicting the final rule to reflect what was outlined in HHS's Dec. 2020 announcement); *see also* Maggie Hales, *Prepare for HIPAA Changes Ahead*, HIPAA E-TOOL, https://thehipaaetool.com/prepare-for-hipaa-changes-ahead/ [https://perma.cc/UL92-4CQD] (last updated July 27, 2023) (stating that the Final Rule is expected to be published in 2023).

access their health records" [177] broadens the safety net, the proposed rule does not include the vast data implicated in text messages, direct messages, search history and geolocation data that remain vulnerable to poaching by law enforcement. Although it should be uncontroversial that "[h]ealth-care data residing outside traditional health-care space" deserves "no less protection than that inside it,"[178] the weak HIPAA construct provides opportunities for law enforcement to obtain reproductive health care data via data from services and products that fall outside any regulatory framework.

B. Digital Breadcrumbs: Free or For Sale

[44] Law enforcement can collect reproductive health care data from the ample breadcrumbs left by digital products and services residing outside the HIPAA framework in two distinct ways: free or for sale. Both ways allow law enforcement to circumvent traditional warrant requirements against individuals. Instead, law enforcement can obtain data for free by issuing warrants, subpoenas or orders against entities that have custody of data; and law enforcement can purchase data that is for sale directly from data brokers.[179]

[45] Crossover exists between data that can be obtained via legal process and data that can be outright purchased, in part because companies can utilize the kinds of tracking systems data brokers use, explained below,[180] and thus could themselves be subject to warrants or subpoenas. Data about online activity is one such example; location data is another. To streamline the discussion, the following categorizes "free" breadcrumbs as those that can be obtained via subpoena because the data is located in a company-

[177] *See* Amick, *supra* note 176.

[178] Terry, *supra* note 16, at 202.

[179] *See* Boodman et al., *supra* note 130.

[180] *See* discussion *infra* Part III.B.2.

owned cloud or server. On the other hand, breadcrumbs "for sale" are data that can be purchased from data brokers who use trackers, including those that market products specifically for law enforcement, and data brokers that harvest data from apps generally.

[46] The Article discusses location data under both categories because of its critical capacity to disclose what reproductive health services may have been sought or obtained. Reproductive health care data thus must include geolocation data even though it is not considered health care data in the traditional sense. Cell phones, which are ubiquitous, are "essentially tracking devices,"[181] and "[t]racking visitors to abortion clinics has long been a staple in showing the threat posed by location data."[182] Moreover, under *Dobbs*, uncertainty arises in gray-zone situations such as where a patient whose home state has banned abortion receives medical abortion medication through the mail or seeks post-abortion medical care via telehealth. Hence, the FTC has described information related to "personal reproductive matters" as "a particularly sensitive subset at the intersection of location and health."[183]

[47] Kavanaugh's concurrence ruling out travel bans that attempt to prevent women from traveling to another state where abortion is legal,

[181] Dellinger & Pell, *supra* note 7.

[182] Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022, 12:46 PM), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood/ [https://perma.cc/7P8E-MUFG].

[183] Kristin Cohen, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, FTC (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal [https://perma.cc/F5CY-7B2J].

"based on the constitutional right to interstate travel,"[184] provides little reassurance. Legislatures in states like Texas and Missouri, with near-total bans on abortion on their books,[185] have started drafting legislation to restrict out-of-state abortions.[186] Texas lawmakers plan to introduce legislation that would, if passed, provide not just civil but criminal penalties for those who travel to another state to obtain an abortion.[187] Because location information can be used to criminalize women post-*Roe*, it is included in this analysis as a critical digital breadcrumb of an individual's reproductive health care data. Section 1 looks at location data that law enforcement can obtain through "free" geofence warrants. Section 2 looks at location data law enforcement can purchase from data brokers.

1. Free: Subpoenas and Orders

[48] Subpoenas are generally easier to obtain than warrants. To search a user's personal electronic device, such as an individual cell phone, law

[184] Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2228, 2309 (2022); *see also* Alan B. Morrison*, No, South Dakota Can't Ban Its Residents From Traveling to Get an Abortion*, SLATE (June 28, 2022, 5:40 PM), https://slate.com/news-and-politics/2022/06/brett-kavanaugh-abortion-travel-ban-dobbs.html [https://perma.cc/V8K3-2SJC].

[185] *See* Eliza Collins, *House Passes Bills Protecting Abortion Access in First Votes After Supreme Court Ruling*, WALL ST. J., https://www.wsj.com/articles/house-set-to-vote-on-bills-protecting-abortion-access-11657896570 [https://perma.cc/GVM7-NLME] (last updated July 15, 2022, 3:30 PM).

[186] *See* Louis Jacobson, *Can states punish women for traveling out of state to get an abortion?*, POLITIFACT (June 29, 2022), https://www.politifact.com/article/2022/jun/29/can-states-punish-women-traveling-get-abortion/ [https://perma.cc/3ZWM-WJT6].

[187] Collins, *supra* note 185.

enforcement must obtain a warrant showing probable cause.[188] However, if that same data is located in the cloud or a server owned by a company, such as a cell phone service provider, social media service or networking platform, or technology company that enables the smart device, a subpoena may suffice in a pending case to direct a witness to produce the data.[189] The moving party only needs to demonstrate that the request for information is relevant, admissible, and specific, *i.e.*, not intended as a general "fishing expedition."[190] Similarly, a court order pursuant to 18 U.S.C. § 2703 of the Stored Communications Act[191] authorizes law enforcement to compel a provider of electronic communication services to disclose certain subscriber records.[192] Such an order can be granted based on a showing of "reasonable grounds to believe" that the records sought are "relevant and material" to

[188] *E.g.,* Riley v. California, 573 U.S. 373, 381–82 (2014) (citing the Fourth Amendment requirement of a warrant supported by probable cause, and particularly describing the place to be searched, and the persons or things to be seized, for a search and seizure to be constitutional). This could also include other individual devices, such as smart watches or computers.

[189] *See* Rina Torchinsky, *How period tracking apps and data privacy fit into a post*-Roe v. Wade *climate*, NPR, https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortionperiod-apps?utm_source=twitter.com&utm_medium=social&utm_term=nprnews&utm_campaign=npr [https://perma.cc/87KD-X37E] (last updated June 24, 2022, 3:06 PM); Christopher Slobogin, *Policing and the Cloud*, NAT'L CONST. CTR., https://constitutioncenter.org/media/files/sloboginfinal5.pdf (last visited Oct. 10, 2023); FED R. CRIM. P. 17(a) ("A subpoena must state the court's name and the title of the proceeding, include the seal of the court, and command the witness to attend and testify at the time and place the subpoena specifies.").

[190] FED. R. CRIM. P. 17(c); United States v. La Rouche Campaign, 841 F.2d 1176, 1178–79 (1st Cir. 1988).

[191] 18 U.S.C. §§ 2701–12.

[192] 18 U.S.C. § 2703(d); *see also* EPIC v. DOJ *(CSLI Section 2703(d) Orders)*, ELEC. PRIV. INFO CTR. https://epic.org/documents/epic-v-doj-csli-section-2703d-orders/ [https://perma.cc/C8PG-LMSX] (last visited Oct. 10, 2023).

an ongoing criminal investigation, also a lower standard than the probable cause requirement of a warrant.[193]

[49] Not only are the standards for obtaining a subpoena or order lower than for a warrant, but data can continue to remain on the cloud or a server even after being deliberately deleted from an individual device or account.[194] Thus, warrants, subpoenas, and orders against the company can allow access to more data than would be accessible via a warrant against an individual's device. The next section addresses data located in the cloud or a server that law enforcement can opt to obtain via warrants, subpoenas, or orders against an entity, specifically seeking an individual's text messages, direct messages, search history, keyword search warrants, and geofence warrants. The purchase of data from data brokers will be discussed in Part 2, which follows.[195]

a. Text Messages, Direct Messages; Search History and Keyword Search Warrants

[50] Even pre-*Dobbs*, law enforcement obtained warrants for an individual's text messages or browsing history for abortion prosecutions.[196] In 2015, for example, Purvi Patel was found guilty of killing her fetus and neglect of a child based on text messages between Patel and a friend that

[193] 18 U.S.C. §2703(d).

[194] James Vincent, *Instagram kept deleted photos and messages on its servers for more than a year*, VERGE (Aug. 14, 2020, 4:28 AM), https://www.theverge.com/2020/8/14/21368602/instagram-kept-deleted-photos-messages-onservers-year-bug-fixed [https://perma.cc/AHF5-R9TX].

[195] *See* discussion *infra* Part III.B.2.

[196] CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, & LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW (2022) [https://perma.cc/3Q93-RVHT] (last updated July 8, 2022).

discussed taking mifepristone to induce an abortion.[197] The appeals court vacated the feticide conviction, finding the law was not meant to be used against women for their own abortions.[198] Most of the 61 investigations in the last two decades against pregnant women or those who aided them in self-managed abortions have been based on statutes not related to abortion.[199] As one policy analyst stated, "[w]hile we've seen local prosecutors prosecute people for managing their own abortions in the past, without Roe in place it's going to become more common."[200]

[51] Post-*Roe*, tech companies can expect to see an upsurge not only in warrants for text messages, as in the *Patel* case, but also direct messaging (DMs) and search histories of individuals who are seeking or have obtained reproductive health care.[201] In July 2023, 18 year-old Celeste Burgess was sentenced to 90 days in jail and two years of probation after entering a guilty plea to a felony charge of concealing or abandoning a dead human body.[202] Celeste and her mother were criminally charged after law enforcement obtained a warrant of all the pair's correspondence on Facebook

[197] *See* Patel v. State, 60 N.E.3d 1041, 1044–46 (Ind. Ct. App. 2016); *see also* Lauren Feiner, Roe v. Wade *overturned: Here's how tech companies and internet users can protect privacy*, CNBC, https://www.cnbc.com/2022/06/24/roe-v-wade-overturned-how-tech-companies-and-users-can-protect-privacy.html [https://perma.cc/JRZ2-UN5V] (last updated June 24, 2022, 1:23 PM).

[198] *Patel*, 60 N.E.3d at 1061–62.

[199] Shaila Dewan & Sheera Frenkel, *A Mother, a Daughter and an Unusual Abortion Prosecution in Nebraska,* N.Y. TIMES (Aug. 18, 2022), https://www.nytimes.com/2022/08/18/us/abortion-prosecution-nebraska.html [https://perma.cc/N9WZ-7WYC].

[200] *Id.* (quoting a state policy analyst for the Guttmacher Institute, a research group that supports abortion rights).

[201] *See, e.g*., Feiner, *supra* note 197.

[202] Andy Rose, *Nebraska woman charged with disposing of fetus following illegal abortion sentenced to 90 days in jail*, CNN (July 20, 2023, 7:53 PM), https://www.cnn.com/2023/07/20/us/nebraska-teen-abortion-celeste-burgess/index.html [https://perma.cc/X68C-GX8M].

Messenger.[203] The search warrant issued to Meta requested the pair's chat history and data including log-in timestamps and photos.[204] Although initially an investigation into the burial and burning of a stillborn baby's remains,[205] the focus shifted when messages appeared to show that the pregnancy had been aborted and not miscarried as the two had claimed.[206] The case "marks one of the first instances of a person's Facebook activity being used to incriminate her in a state where abortion access is restricted."[207]

[52] Most major tech companies' longstanding policy is to comply with valid warrants.[208] While true that Meta and similar companies do have to comply with legal requests for data, one protection would be to cease collecting certain kinds of data in the first place.[209] The data then would not exist on company servers, preventing law enforcement from obtaining it

[203] Dewan & Frenkel, *supra* note 199.

[204] James Vincent, *Facebook turns over mother and daughter's chat history to police resulting in abortion charges*, VERGE (Aug. 10, 2022, 6:51 AM), https://www.theverge.com/2022/8/10/23299502/facebook-chat-messenger-history-nebraska-teen-abortion-case [https://perma.cc/L8XJ-L8Q6].

[205] Dewan & Frenkel, *supra* note 199.

[206] 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/L3SL-8AGR].

[207] Emily Baker-White & Sarah Emerson, *Facebook Gave Nebraska Cops A Teen's DMs. They Used Them to Prosecute Her For Having An Abortion*, FORBES (Aug. 8, 2022, 9:23 PM), https://www.forbes.com/sites/emilybaker-white/2022/08/08/facebook-abortion-teen-dms/?sh=2cacacb5579c [https://perma.cc/STA4-R45A].

[208] Kaste, *supra* note 206.

[209] Vincent, *Facebook*, *supra* note 204.

without a warrant against the specific individual targeted by the search.[210] WhatsApp, for example, encrypts messages end-to-end (E2EE).[211] Had E2EE also been the default setting for messages on Facebook Messenger, the police would have been required to gain direct access to Celeste's and Jessica's phones to read their chats.[212]

[53] In addition to texts and chats, indictments have been based on reproductive health care search histories, which can be "incredibly telling if an individual is considering or seeking an abortion."[213] For example, two years after the *Patel* case, in 2017, at a medical facility in Mississippi where Latice Fisher arrived with her stillborn fetus, medical staff immediately treated her with suspicion of committing a crime.[214] Prosecutors used Fisher's search history, which included queries on how to induce a miscarriage and purchase abortion pills online, as evidence against her,

[210] *Id.*

[211] *Id.*

[212] *Id.*

[213] Kewa Jiang, *Data Privacy Risks in a Potential Post*-Roe v. Wade *World*, CAL. LAWYERS ASS'N (June 16, 2022), https://calawyers.org/privacy-law/data-privacy-risks-in-a-potential-post-roe-v-wade-world-by-kewa-jiang/ [https://perma.cc/9J9T-BLXG].

[214] Cynthia Conti-Cook, *supra* note 7, at 3–4.

though the district attorney eventually dropped the second-degree murder charge.[215]

[54] Similarly, in 2019, prosecutors presented Brooke Skylar Richardson's browsing history during a trial in which she stood accused of killing and burying her newborn baby.[216] While defense attorneys said the baby was stillborn, prosecutors' argument that Richardson had killed the infant relied in part on her internet query, "how to get rid of a baby."[217] Similar to Fisher, against whom charges were dropped, Richardson ultimately was acquitted of murder and manslaughter charges.[218]

[55] Even more broad than the particularized warrant used against Fisher and Richardson is a warrant known as the "keyword warrant," sometimes referred to as a "reverse keyword search warrant."[219] Rather than starting with an individual, the warrant allows law enforcement to "start with a search term of interest and identify users who have searched it within a

[215] Feiner, *supra* note 197; *see* Nicole Nguyen & Cordilia James, *How Period-Tracker Apps Treat Your Data, and What That Means if* Roe v. Wade *is Overturned*, WALL ST. J., https://www.wsj.com/articles/how-period-tracker-apps-treat-your-data-and-what-that-means-if-roe-v-wade-is-overturned-11655561595 [https://perma.cc/C4DB-8VNV] (last updated June 21, 2022, 12:00 AM); *see also* Isha Marathe, *Post-'Dobbs,' Privacy Attorneys Prepare for Increased Data Surveillance*, LEGALTECH NEWS (June 27, 2022, 5:31 PM), https://www.law.com/legaltechnews/2022/06/27/post-dobbs-privacy-attorneys-prepare-for-increased-data-surveillance/ [https://perma.cc/29B6-EXDB] [hereinafter Marathe, Post-'Dobbs']; *Why data privacy is a concern in the wake of* Roe v. Wade *reversal*, CBS NEWS (June 29, 2022, 5:40 PM), https://www.cbsnews.com/news/abortion-ban-surveillance-tracking-technology/ [https://perma.cc/4KGV-BNH9].

[216] *Why Data Privacy is a Concern in the Wake of* Roe v. Wade *Reversal*, *supra* note 215.

[217] *Id.*

[218] *Id.*

[219] *See id.*; *see also* Corin Faife, *Powerful keyword warrants face new challenge in deadly arson case*, VERGE (July 1, 2022, 12:39 PM), https://www.theverge.com/2022/7/1/23191406/denver-arson-google-keyword-warrant-challenge-constitutional-fourth-amendment-privacy [https://perma.cc/X7BW-95RF].

particular period."[220] The technique has been described as a "fishing expedition" for information on "everyone who has Googled specific search terms,"[221] including search terms such as "abortion drugs."[222] A group of civil rights organizations, concerned about reverse keyword warrants' invasiveness, has asked Google to provide greater transparency on how law enforcement agencies request data using keyword and geofence warrants, arguing that "[t]hese blanket warrants circumvent constitutional checks on police surveillance . . . ."[223]

[56] One such keyword search warrant, used together with other surveillance methods, led law enforcement to suspects in an arson case in Colorado.[224] An attorney representing a defendant identified through a keyword warrant argued to suppress all evidence derived from the warrant:

> A reverse keyword search is a novel and uniquely intrusive digital dragnet of immense proportions. . . . No court has considered the legality of a reverse keyword search, but its constitutional defects are readily apparent and should have been obvious to all involved. It is a 21st century version of the general warrants that the Fourth Amendment was designed to guard against. Just as no warrant could authorize

[220] Faife, *supra* note 219.

[221] 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/8XJM-76FZ].

[222] Faife, *supra* note 219.

[223] *Id.*; *see generally* Zachary Schapiro, Note, *Data Protection in the Digital Economy: Legislating in Light of* Sorrell v. IMS Health Inc., 63 B. C. L. REV. 2007, 2007 (2022); *see generally* Motion to Suppress Evidence from a Keyword Warrant & Request for a Veracity Hearing at 1, People v. Seymour, 526 P3.d 954 (Colo. Jan. 17, 2023), https://s3.documentcloud.org/documents/22076537/motion-to-suppress-google-evidence-in-colorado-vs-seymour.pdf [https://perma.cc/6E7M-5J2F].

[224] Faife, *supra* note 219.

> the search of every home in America, no warrant can compel a search of everyone's Google queries.[225]

[57] However, the district court judge upheld the warrant's legality, and the issue was argued before the Colorado Supreme Court.[226] The case was one of first impression not only in Colorado, but nationally.[227] The Electronic Frontier Foundation filed an amicus brief urging that the reverse keyword warrant is overbroad and violates both the Colorado state and U.S. constitutions.[228] The case tests law enforcement's ability to investigate and criminalize an individual based on "googling" history, because "[s]earch engines are an indispensable tool for finding information on the Internet, and the right to use them—and use them anonymously—is critical to a free society."[229]

---

[225] Motion to Suppress Evidence from a Keyword Warrant & Request for a Veracity Hearing, *supra* note 223 at 1–2.

[226] Shelly Bradbury, *Court hears first-of-its-kind challenge to police's use of Google search terms to ID murder suspects*, L.A. DAILY NEWS, https://www.dailynews.com/2023/05/05/google-reverse-keyword-search-warrant-colorado-supreme-court-arguments/ [https://perma.cc/56EN-XW88] (last updated May 5, 2023, 7:53 AM); Liana Kramer, *Reverse keyword search warrant used to identify suspects in fatal arson case goes to Colorado Supreme Court*, COLO. NEWS (Jan. 22, 2023), https://localtoday.news/co/reverse-keyword-search-warrant-used-to-identify-suspects-in-fatal-arson-case-goes-to-colorado-supreme-court-news-92977.html [https://perma.cc/A865-WC2R].

[227] Brief for Petitioner-Juvenile Defendant at 5, Seymour v. Colorado, No. 2023SA12 (Colo. Jan. 11, 2023).

[228] Jennifer Lynch & Andrew Crocker, *UPDATE: Colorado Supreme Court Grants Review in First U.S. Case Challenging Dragnet Keyword Warrant*, ELEC. FRONTIER FOUND., https://www.eff.org/deeplinks/2022/06/eff-file-amicus-brief-first-us-case-challenging-dragnet-keyword-warrant [https://perma.cc/9MAT-QEFK] (last updated Jan. 18, 2023).

[229] *See id.*

b. Geofence Warrants

[58] Like keyword warrants, geofence warrants start with data searches to identify individuals, in contrast to traditional warrants that start with an identified individual whose data is then searched.[230] Because they work backward, geofence warrants are also sometimes called reverse location warrants.[231] Reverse warrants allow law enforcement to identify cell phone users at the time and geographic location where the crime occurred within a "geofence," a map of geolocation coordinates law enforcement specifies for the warrant.[232] GPS or radio frequency identification can determine a device's location within such a geofence boundary.[233] The broad search range of geofence warrants "grants law enforcement permission to obtain anonymized data from a data aggregator like Google, on every location-trackable device in a specific radius at a specific time."[234]

[59] The over-inclusivity of reverse warrants poses a Fourth Amendment challenge that courts so far have not dealt with extensively.[235] Concerned that Google collects "detailed swaths of location data from their users," the federal district court in *United States v. Chatrie* observed generally that

---

[230] *See* Isha Marathe, *Despite Rulings, 4th Amendment Battles Over GeoFence Warrants Are Far From Over,* LEGAL TECH NEWS, (May 26, 2022, 4:45 PM), https://www.law.com/legaltechnews/2022/05/26/despite-rulings-fourth-amendment-battles-over-geofence-warrants-are-far-from-over/ [https://perma.cc/85GQ-KD84] [hereinafter Marathe, *4th Amendment*].

[231] *See id.*

[232] *In re* Search of Info. That is Stored at the Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 67–69 (D.D.C. 2021).

[233] Marathe, *Post-'Dobbs,' supra* note 215.

[234] Marathe, *4th Amendment*, *supra* note 230.

[235] *In re Search of Info.*, 579 F. Supp. 3d at 67–69 ("Though geofence warrants raise a number of important constitutional questions, there is not much federal caselaw discussing their legality.").

"[l]aw enforcement has seized upon the opportunity presented by this informational stockpile, crafting 'geofence' warrants that seek location data for every user within a particular area over a particular span of time."[236] The court accordingly held that the specific geofence warrant at hand was unconstitutional.[237] Since the warrant sought location information for all Google account holders who entered the warrant's flagged area within the specified hour, it failed to establish individualized probable cause.[238] Unlike a user's visit to a website featuring child pornography to establish probable cause, "a Google user's proximity to the bank robbery does not necessarily suggest that the user participated in the crime."[239] However, the *Chatrie* court carefully declined to take a position on "whether a geofence warrant may *ever* satisfy the Fourth Amendment's strictures."[240]

[60] Other courts have found geofence warrants to be constitutional, on seemingly broad criteria applicable to many contexts. For example, in *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, the district court found "that the government's application for location data within six geofence areas relating to an arson investigation satisfie[d] the probable cause and particularity requirements of the Fourth Amendment."[241] Not only did the court find that "ample probable cause" existed that the crimes of arson and

[236] United States v. Chatrie, 590 F. Supp. 3d 901, 905 (E.D. Va. 2022).

[237] *Id.*

[238] *Id.* at 929.

[239] *Id.* at 931.

[240] *Id.* at 932.

[241] *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F.Supp.3d 345, 349 (N.D. Ill. 2020).

conspiracy to commit arson occurred,[242] but that there is "also probable cause that evidence of the crime will be located at Google because location data on cell phones at the scene of the arson, as well as the surrounding streets, can provide evidence on the identity of the perpetrators and witnesses to the crime."[243] Similarly, in *In re Search of Information That is Stored at the Premises Controlled by Google LLC*, the court found probable cause "that the search will produce evidence useful to the government's investigation of the criminal activity in question" because of the "'fair probability' that (i) the suspects were inside the geofence, (ii) were using their cell phones inside the geofence, (iii) those phones communicated location information to Google, and (iv) Google can trace the information back to a particular device, accountholder, and/or subscriber."[244]

[242] *Id.* at 354–55 ("As the facts supplied by the affidavit demonstrate, there is a fair probability that the fire was set maliciously*, i.e.* intentionally, by multiple persons in coordination, on vehicles that are stored in commercial businesses on multiple dates.").

[243] *Id.* at 355–56.

[244] *In re* Search of Info. That is Stored at the Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 79 (D.D.C. 2021); *but see In re* Search of Info. That is Stored at the Premises Controlled by Google, LLC, 542 F. Supp. 3d 1153, 1154, 1156-57 (D. Kan. 2021) (holding that the geofence warrant for an area that surrounds and includes a building where a federal crime allegedly occurred was "not sufficiently specific or narrowly tailored to establish probable cause or particularity." Although the application "establishes probable cause that a crime was committed at the subject business establishment during the relevant one-hour time period . . . it does not establish probable cause that evidence of the crime will be located at the place searched—that is, Google's records showing the location data of cell phone users within the geofence boundaries." Not only does the affidavit fail to demonstrate a fair probability "that any pertinent individual would have been using a device that feeds into Google's location-tracking technology," but "[t]he application also does not address the anticipated number of individuals likely to be encompassed within the targeted Google location data. . . . If a geofence warrant is likely to return a large amount of data from individuals having nothing to do with the alleged criminal activity . . . the sheer amount of information lessens the likelihood that the data would reveal a criminal suspect's identity, thereby weakening the showing of probable cause.").

[61] The lack of a consistent standard for the constitutionality of a geofence warrant leaves wide open the possibility that geofence warrants can be issued "to identify people who were in or around" abortion clinics.[245]

[62] In the meantime, courts are issuing geofence warrants at increasing rates.[246] The *Chatrie* court noted that Google alone received its first geofence warrant in 2016; from 2017 to 2018 Google "observed over a 1,500% increase in the number of geofence requests it received"; and that geofence warrants now "comprise more than twenty-five percent of *all* warrants it receives in the United States."[247] In addition to Google, geofence warrants have been issued to Apple, Uber, and Snapchat.[248]

[63] Alarmed by the upsurge in "dragnet 'geofence' orders demanding data about everyone who was near a particular location at a given time," with law enforcement "routinely" requesting such information from Google, members of Congress wrote a letter to Google in May 2022.[249] The senators requested that the company "stop unnecessarily collecting and retaining customer location data, to prevent that information from being

[245] Jiang, *supra* note 213.

[246] Marathe, *4th Amendment*, *supra* note 230; Sidney Fussell, *An Explosion in Geofence Warrants Threatens Privacy Across the US*, WIRED (Aug. 27, 2021, 6:19 PM), https://www.wired.com/story/geofence-warrants-google/ [https://perma.cc/FL25-8UCM] ("New figures from Google show a tenfold increase in the requests from law enforcement, which target anyone who happened to be in a given location at a specified time.").

[247] United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022) (emphasis in original).

[248] Fussell, *supra* note 246.

[249] Letter from 42 members of Congress to Sundar Pichai, Google Chief Exec. Officer (May 24, 2022), https://www.wyden.senate.gov/imo/media/doc/Wyden-led%20letter%20to%20Google%20on%20geofence%20data%20and%20abortion-related%20surveillance%205.24.22.pdf [https://perma.cc/MKL9-HW79].

used . . . to identify people who have obtained abortions."[250] Google has since attempted to address some of the privacy concerns by pledging that if its systems identify that a customer has visited an abortion clinic or fertility center, Google will delete those entries from Location History "soon after [they] visit."[251]

[64] Concerns about tracking women by location history have already led Massachusetts to curtail geolocation collection near abortion clinics.[252] In 2017, the Massachusetts Attorney General reached a settlement with a digital advertising company hired to use mobile geofencing technology "to identify when people crossed a secret digital 'fence' near a clinic offering abortion services."[253] Based on that data, the company had been sending targeted ads to those individuals' phones with links to websites with information about abortion alternatives, a practice the Massachusetts Attorney General asserted violated state consumer protection law.[254] Currently, Massachusetts is the only state that bans geolocation near abortion clinics.[255] In the meantime, with the courts inconsistent and other

[250] *Id.*; *see also* Dellinger & Pell, *supra* note 7.

[251] Jen Fitzpatrick, *Protecting people's privacy on health topics*, GOOGLE (May 12, 2023), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/ [https://perma.cc/W2KF-9BNT].

[252] Marathe, *Post-* 'Dobbs,' *supra* note 215

[253] Jonathan Greig, *FTC puts data collectors and brokers on notice in light of abortion bans,* THE RECORD (July 12, 2022), https://therecord.media/ftc-puts-data-collectors-and-brokers-on-notice-in-light-of-abortion-bans [https://perma.cc/59J2-P3WL].

[254] Press Release, Office of Attorney General Maura Healey, AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities (Apr. 4, 2017), https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities [https://perma.cc/2Y97-WM7A]; Cohen, *supra* note 183.

[255] Marathe, *Post-* 'Dobbs,' *supra* note 215.

state legislatures so far silent on their legality, geofence warrants remain a potent tool for law enforcement.

2. For Sale: Data Brokers

[65] On the other hand, law enforcement does not need to serve legal process upon an entity if it can purchase the data instead from a data broker. Data brokers can collect data from both websites and apps, in which trackers are embedded that collect and send data to data brokers.[256] Websites use a cookie, a small text file that websites put on a computer that allows sites to remember preferences about pages and functions used in the browser.[257] Mobile apps, on the other hand, rely on software development kits, or SDKs, that data brokers embed in the apps.[258]

[66] Data brokers provide SDKs to app developers for free in exchange for the data the apps collect or a portion of the ad revenue, and these SDKs enable conveniences for the mobile app's users, such as the sign-in feature for Facebook.[259] SDKs like Facebook's also allow apps to collect data in

[256] Zack Whittaker, *Data brokers track everywhere you go, but their days may be numbered*, TECHCRUNCH (July 9, 2020, 9:00 AM), https://techcrunch.com/2020/07/09/data-brokers-tracking/ [https://perma.cc/H8YF-MRBN].

[257] *Delete and manage cookies*, MICROSOFT, https://support.microsoft.com/en-us/windows/delete-and-manage-cookies-168dab11-0753-043d-7c16-ede5947fc64d [https://perma.cc/M53F-HZ8T] (last visited Mar. 27, 2023).

[258] 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/UF7C-SU9H].

[259] *See id.*; Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J., (Feb. 22, 2019, 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 [https://perma.cc/NY9Q-GQ82]; Sara Morrison, *The hidden trackers in your phone, explained*, VOX (July 8, 2020, 10:30 AM), https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location [https://perma.cc/LT2B-KW3J].

order to sell advertising targeted to the user's interests.[260] In contrast to cookies on a website, apps by definition reside on a device such as a cell phone that is carried around all day, allowing SDKs to collect immense amounts of information.[261] Thus, in return for providing valuable information or convenience, the data brokers are able to collect information through the app that they can sell to advertisers; take a percentage of the ads the app sells; or resell the data to yet other data brokers.[262]

[67] Not only do SDKs harvest real-time location data from smartphone apps that one expects to request location permissions, such as weather apps, navigation apps, digital maps, and rideshare services, but they also harvest from less obvious apps like coupon apps that "enable key features."[263] Such mobile apps track users' movements "with great precision and frequency."[264] Once installed, an SDK has access to location data whenever

[260] Schechner & Secada, *supra* note 259.

[261] Morrison, *supra* note 259.

[262] *Id.*; *see* Whittaker, *supra* note 256; *see also* Cyphers, *supra* note 258.

[263] *See* Cyphers, *supra* note 258; *see also* Jiang, *supra* note 213 (Social media platforms can also collect data on the precise geolocation of its users, not to mention that "[t]he very smartphone on which all these apps reside is also one of the greatest sources of precise geolocation information."); *see generally* Christopher Mims, *Your Location Data Is Being Sold—Often Without Your Knowledge*, WALL ST. J. (Mar. 4, 2018), https://www.wsj.com/articles/your-location-data-is-being-soldoften-without-your-knowledge-1520168400 [https://perma.cc/UH7P-88EE] (describing how "WeatherBug," one of the most popular weather apps for Android and iPhone, is owned by the location advertising company GroundTruth: "It's a natural fit: Weather apps need to know where you are and provide value in exchange for that information. But it also means that app is gathering data on your location any time the app is open—and even when it isn't, if you agreed to always let it track your location. That data is resold to others. . . . App makers agree to harvest location data because it grants them access to GroundTruth's mobile advertising network. . . . Every month GroundTruth tracks 70 million people in the U.S. as they go to work in the morning, come home at night, surge in and out of public events, take vacations, you name it.").

[264] Cyphers, *supra* note 258.

the app is open, but also may have "'background' access to data . . . even if the app is closed."[265] By collecting location data, including where a phone is usually located at night, a data broker may be able to calculate where visitors to a location, such as a Planned Parenthood clinic, "live to the census block level." [266]

[68] In sum, the SDK ecosystem and the resulting data flows are diverse and complex,[267] with SDKs providing "the mobile equivalent of cookies . . . , but with more power."[268] Post-*Roe*, reproductive health data, whether collected via cookies or SDKs, will become even more valuable to data brokers.[269]

[69] This discussion focuses on two categories of law enforcement data collection: first, via technologies designed specifically for law enforcement;[270] second, via purchase from general data brokers.[271]

---

[265] *Id.*

[266] Cox, *supra* note 182.

[267] *See* Morrison, *supra* note 259 (statement of Professor Norman Sadeh, director of Carnegie Mellon University's Mobile Commerce Laboratory and e-Supply Chain Management Laboratory, and co-director of its MSIT-Privacy Engineering Program) ("This ecosystem [of SDKs] has become extremely complex, and the data flows that result from all this are extremely diverse and very, very concerning.").

[268] *Id.* (quoting Whitney Merrill, a privacy lawyer).

[269] Amanda James, *Following* Roe *decision, bad actors will try to target reproductive health data,* MEDCITY NEWS (June 24, 2022, 3:32 PM), https://medcitynews.com/2022/06/following-roe-decision-bad-actors-will-try-to-target-reproductive-health-data/ [https://perma.cc/AJ7X-VA5M] (quoting a lawyer who works with FemTech companies).

[270] Cyphers, *supra* note 258.

[271] *Id.*

a. Data Collection for Law Enforcement

[70] Law enforcement agencies collect and compile vast databases of personal information via tools such as automated license plate readers, cell-site simulators, drones or unmanned aerial vehicles, and face recognition systems.[272] Indeed, "law enforcement agencies are following closely behind their counterparts in the military and intelligence services in acquiring privacy-invasive technologies."[273] This Article identifies three broad types of law enforcement-focused data collection systems: (1) those that scrape data from social media posts; (2) others that harvest data from mobile apps; and (3) a final category that captures data from installed monitoring systems.

i. Technologies that Scrape Data from Social Media

[71] Clearview AI is a prominent example of a technology marketed specifically to law enforcement that scrapes data from public social media posts.[274] Clearview "built its facial recognition software by scraping photos from the web and popular sites"[275] which it then packaged into software for law enforcement,[276] without consent from either the websites or those

[272] *A Guide to Law Enforcement Spying Technology*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/street-level-surveillance [https://perma.cc/LTP6-462A] (last visited Oct. 2, 2023).

[273] *Id.*

[274] *Introducing Clearview AI 2.0*, CLEARVIEW AI (Mar. 24, 2022), https://www.clearview.ai/post/introducing-clearview-ai-2-0 [https://perma.cc/T2KM-XLAR].

[275] Ryan Mac & Kashmir Hill, *Clearview AI settles suit and agrees to limit sales of facial recognition database*, N.Y. TIMES (May 9, 2022), https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html [https://perma.cc/TFU4-TVYS].

[276] *Id.* (noting that Clearview sold its software to "local police departments and government agencies, including the F.B.I. and Immigrations and Customs Enforcement.").

photographed.[277] Anyone whose image is on Facebook, Google, LinkedIn, Instagram, Twitter, or YouTube, for example, may already be part of Clearview AI's database. Clearview's website states that its database includes over 30 billion images.[278] The company's "cavalier approach to data harvesting"[279] led the American Civil Liberties Union to file a lawsuit in Illinois under the Biometric Information Privacy Act.[280] Clearview agreed to ban most private entities from using its database and is barred from selling access to Illinois entities, including government agencies, for five years.[281] The terms of the May 2022 settlement, however, still allow law enforcement agencies outside Illinois with a subscription to Clearview AI to utilize the faceprint database.[282]

ii. Technologies that Harvest Data from Mobile Apps

[72] Other companies specifically sell location data harvested from mobile apps to federal law enforcement and government contractors.[283]

[277] Drew Harwell, *Facial recognition firm Clearview AI tells investors it's seeking massive expansion beyond law enforcement*, WASH. POST (Feb. 16, 2022, 12:47 PM), https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/ [https://perma.cc/R29E-R9QA].

[278] *See generally* CLEARVIEW AI, https://www.clearview.ai/ [https://perma.cc/7YR4-UAUA] (last visited Oct. 12, 2023).

[279] Harwell, *supra* note 277.

[280] Mac & Hill, *supra* note 275.

[281] *ACLU v. Clearview AI*, ACLU (May 11, 2022), https://www.aclu.org/cases/aclu-v-clearview-ai [https://perma.cc/824Z-7PBU]; Mac & Hill, *supra* note 275.

[282] Adi Robertson, *Clearview AI agrees to permanent ban on selling facial recognition to private companies*, VERGE (May 9, 2022, 2:59 PM), https://www.theverge.com/2022/5/9/23063952/clearview-ai-aclu-settlement-illinois-bipa-injunction-private-companies [https://perma.cc/SM2F-8HAK].

[283] Cyphers, *supra* note 258.

While they may have futuristic names, these companies are already in our midst: Venntel; Babel Street, with its flagship product, Babel X; Anomaly 6 ("A6"); and X-Mode.[284]

[73] As an example, Venntel harvests location data from smartphone apps.[285] Its "proprietary platform analyzes billions of commercially-available location signals to provide insight into digital device locations and movement patterns."[286] Using data analytics, Venntel aggregates this location data into its software product for government agencies like the Department of Homeland Security, the IRS's criminal investigation division, and the FBI.[287] Another system called Fog Reveal, which the Electronic Frontier Foundation found draws its data from Venntel, provides location data at a discounted rate to state and local law enforcement, who are able to run area searches that resemble geofence warrants, as well as individual device searches.[288] These platforms enable law enforcement to

[284] *Id.*

[285] *Id*.; Kim Lyons, *Congress investigating how data broker sells smartphone tracking info to law enforcement*, VERGE (June 25, 2020, 2:55 PM), https://www.theverge.com/2020/6/25/21303190/congress-data-smartphone-tracking-fbi-security-privacy [https://www.theverge.com/2020/6/25/21303190/congress-data-smartphone-tracking-fbi-security-privacy].

[286] *See generally* Shreya Tewari & Fikayo Walter-Johnson, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data*, ACLU (July 18, 2022), https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data [https://perma.cc/G3GZ-HEGR]; *Our Solutions*, VENNTEL, https://www.aclu.org/sites/default/files/field_document/production_3_reprocessed_jan._22.pdf [https://perma.cc/N53U-5F8R] (last visited July 20, 2022) (internal reference to Venntel marketing brochure).

[287] *See* Cyphers, *supra* note 258; *see also* Lyons, *supra* note 285.

[288] Ashley Belanger, *Cops wanted to keep mass surveillance app secret; privacy advocates refused*, ARS TECHNICA (Sept. 1, 2022, 6:56 PM), https://arstechnica.com/tech-policy/2022/09/cops-wanted-to-keep-mass-surveillance-app-secret-privacy-advocates-refused/ [https://perma.cc/F5GX-6LYY].

conduct sweeps of location data to identify individuals who may have sought information or services at abortion clinics.

iii. Technologies that Capture Data from Installed Monitoring Systems

[74] Finally, location information can be captured by traditional security or monitoring systems. Now, however, these systems are amplified by artificial intelligence. Flock Safety touts its "AI and machine-learning powered technology" that will "give[] you detailed information that you may not have otherwise." [289] Its website states that its automated license plate readers use "a unique Vehicle Fingerprint feature" in which "information is then automatically made searchable, categorized, and stored for fast and easy access later."[290] Similarly, Motorola Solutions' License Plate Recognition platform uses cameras and data analytics to "[h]eighten awareness on the road, guide officer patrol efforts and collect data at scale with powerful, reliable mobile license plate recognition."[291] Like the HIPAA exceptions whose purpose was to protect the patient, Flock Safety's

[289] FLOCK SAFETY, https://www.flocksafety.com/why-flock (last visited Nov. 18, 2023). *See* Mike Johnson, Chino Police Dep't Organized Retail Theft Prevention Grant Program Application to Bd. of State and Cmty. Corr. (July 7, 2023), https://www.bscc.ca.gov/wp-content/uploads/13-Chino-Police-Dept.pdf [https://perma.cc/RZ9A-TVZN].

[290] *Neighborhood Security Guide*, FLOCK SAFETY, https://www.flocksafety.com/resources/neighborhood-security-guide [https://perma.cc/FLX8-3GKA] (last visited Oct. 14, 2023) (elaborating on how one can find a suspect by searching for visual evidence (vehicle make, type, and color, license plate, and unique features) as well as contextual evidence (timestamp, number of times this vehicle has been seen in the last 30 days, and associated vehicles)). *See* Kevin Deutsch, *Margate Police Plan to Install 14 License Plate Surveillance Cameras Throughout City*, MARGATE TALK (Aug. 31, 2022), https://margatetalk.com/margate-police-plan-to-install-license-plate-12071 [https://perma.cc/8KD8-QT4K].

[291] *See generally Mobile License Plate Recognition*, MOTOROLA SOLUTIONS, https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems.html [https://perma.cc/8YG4-4FMN] (last visited Mar. 29, 2023).

and Motorola Solutions' common mission of promoting public safety is laudable. It is the potential for abuse, however, that raises the specter of the surveillance state, including for women seeking reproductive health care post-*Roe*.

b. General Data Collection

[75] In addition to data collected specifically for law enforcement, law enforcement can purchase data from the general data broker market. The following looks at two kinds of data pertinent to reproductive health care collected by general data brokers: location data, and data harvested from fertility apps.

i. Location

[76] The highly profitable data broker ecosystem motivates "companies . . . to share data at an unprecedented scale and granularity."[292] The data is used to develop profiles and draw inferences about a consumer that is monetized.[293] A profile may even be sold auction-style via real-time bidding, and the highest bidders can be any third party, not just advertisers, but also governmental agencies.[294] In addition to one's religious beliefs, sexual orientation, political affiliation, gender, age, education level, and debt, the user profile is also likely to include a particularly sensitive item

[292] Cohen, *supra* note 183 ("According to the [FTC 2014 study], one data broker bragged to shareholders in a 2013 annual report that it had 3,000 points of data for nearly every consumer in the United States.").

[293] *Id.* ("After it's collected from a consumer, data enters a vast and intricate sales floor frequented by numerous buyers, sellers, and sharers . . . These companies often build profiles about consumers and draw inferences about them based on the places they have visited. The amount of information they collect is staggering.").

[294] *See* Angela Doughty & Mayukh Sircar, *Going Once, Going Twice, Sold: Real Time Bidding Data Privacy Breach*, JD SUPRA (July 11, 2022), https://www.jdsupra.com/legalnews/going-once-going-twice-sold-real-time-7645080/ [https://perma.cc/G333-XMJP].

post-*Roe*: location.[295] Data broker companies make "billions of dollars" selling location data alone to the private market.[296]

[77] One company, INRIX, has been selling location-based data analytics for over 17 years.[297] Even the free trial version of the INRIX IQ Location Analytics platform allows a user to "locate at least 71 Planned Parenthood clinics in numerous states," while the paid version "shows more detailed statistics for sample points of interests in its database, including demographic and ethnic breakdowns of visitors, visitor counts by hour and day, aggregated heat maps of the origins and destinations for visitors, and drive times to and from the business location."[298]

[78] In sum, "a vast array of mobile apps" unrelated to health such as "digital maps, rideshare services, and social media platforms" may nonetheless implicate reproductive health choices by revealing the geolocation, for example, of a user at a family planning clinic.[299] At least one data broker has been openly selling location data of people visiting such clinics, "showing where groups of people visiting the locations came from,

[295] *Id.*; *see also* Morrison, *supra* note 259 (explaining that location data has been sold to law enforcement in the past to enforce immigration laws).

[296] Cyphers, *supra* note 258.

[297] Kathryn Rattigan, *Location Data Industry Under Scrutiny for Inclusion of Planned Parenthood Clinics in Their Services*, JD SUPRA (July 22, 2022), https://www.jdsupra.com/legalnews/location-data-industry-under-scrutiny-9465581/ [https://perma.cc/7GBJ-67KC].

[298] *Id.*

[299] *See* Jiang, *supra* note 213; *see also* Torchinsky, *supra* note 189 ("If someone is sitting in the waiting room of a clinic that offers abortion services and is playing a game on their phone, that app might be collecting location data.").

how long they stayed there, and where they then went afterwards."[300] Thus, law enforcement can obtain the very same location data that *Carpenter* and *Chatrie* held require a warrant based on probable cause to access [301] simply by paying data brokers instead.[302]

ii. Fertility Apps

[79] The opaque, unregulated marketplace of data brokers includes mobile health apps, which overtly generate health data yet are not tied to "covered entities" and are therefore left unprotected by HIPAA.[303] Post-*Roe*, fertility apps occupy a conspicuous position among the many mobile health apps as a privacy vulnerability.[304] Such apps allow users to record menstrual cycle dates and predict ovulation and fertility, "serv[ing] as digital diaries for sexual activity, birth control methods and conception attempts. Some women use the apps when they are trying to get pregnant, others to avoid it and many just to know when their next period is

[300] Cox, *supra* note 182 (noting "The sale of the location data raises questions around why companies are selling data based on abortion clinics specifically, and whether they should introduce more safeguards around the purchase of that information, if be selling it at all.").

[301] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018); United States v. Chatrie, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022).

[302] *See* Cyphers, *supra* note 258 ("The federal government cannot do an end-run around these basic Fourth Amendment rules through the stratagem of writing a check to location data brokers.").

[303] *Supra* Part III.A.2; Eric Reicin, *Protecting Consumer Health Data Privacy Beyond HIPAA*, FORBES (May 10, 2022, 7:00 AM), https://www.forbes.com/sites/forbesnonprofitcouncil/2022/05/10/protecting-consumer-health-data-privacy-beyond-hipaa/?sh=19842c7c7b4e [https://perma.cc/N287-Z4R4]; *see also* Cohen, *supra* note 183 (regarding harms to consumer from user-generated health data).

[304] *See* Kim, *supra* note 7.

coming."[305] Since any information shared on the app may also be shared with the data broker who embedded an SDK,[306] the intimate personal health data could reach far beyond the individual user's device or even the app and be used for prosecuting abortions.[307] Post-*Roe*, fear has grown that information on fertility apps could be shared with third parties to criminally implicate a user,[308] and reproductive and privacy rights advocates have urged women to delete the apps.[309] Moreover, while some fertility apps store data locally on the user's device and do not allow third party tracking, other apps commonly store users' data in the cloud[310] or allow tracking, raising concerns that law enforcement could obtain this data via subpoena, as

[305] Kashmir Hill, *Deleting Your Period Tracker Won't Protect You*, N.Y. TIMES, https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html [https://perma.cc/7V64-XSDA] (last updated June 22, 2023).

[306] Schechner & Secada, *supra* note 259; *see also* Cyphers, *supra* note 258.

[307] *See* Torchinsky, *supra* note 189.

[308] *Id.* (statement of Lydia X. Z. Brown) ("We're very concerned in a lot of advocacy spaces about what happens when private corporations or the government can gain access to deeply sensitive data about people's lives and activities . . . . Especially when that data could put people in vulnerable and marginalized communities at risk for actual harm.").

[309] Julia Ries, *Should You Delete Your Period-Tracking App to Protect Your Privacy?*, HEALTH (July 5, 2022), https://www.health.com/news/should-you-delete-period-tracking-app [https://perma.cc/SUE2-AD86]; Hannah Norman & Victoria Knight, *Should You Worry About Data From Your Period-Tracking App Being Used Against You?*, KFF HEALTH NEWS (May 13, 2022), https://khn.org/news/article/period-tracking-apps-data-privacy/ [https://perma.cc/AU89-4VDB] ("'If you are using an online period tracker or tracking your cycles through your phone, get off it and delete your data,' activist and attorney Elizabeth McLaughlin said in a viral tweet. 'Now.'").

[310] *E.g.*, Catherine Roberts, *These Period Tracker Apps Say They Put Privacy First. Here's What We Found.*, CONSUMER REPS., https://www.consumerreports.org/health-privacy/period-tracker-apps-privacy-a2278134145/ [https://perma.cc/HT2F-YRPA] (last updated Aug. 30, 2022).

discussed above.[311] The COVID-19 pandemic accelerated the health industry's expansion into digital health and remote care, and mobile health apps are more popular than ever.[312] Flo, one of the most popular health apps on the market, is a period and fertility-tracking app with more than 48 million active users.[313] Other popular apps that can track fertility cycles include Clue; Fitbit's fitness app, Glow; and Natural Cycles.[314]

[80] Even before *Dobbs*, Flo Health Inc., the developer of the Flo app, had settled with the FTC in 2021 over allegations that it improperly shared personal data, including whether users were ovulating or intended to get

[311] *See* Deborah Gersh et al., *Post*-Dobbs *HHS Guidance Brings Privacy Considerations*, LAW360 (July 29, 2022, 6:44 PM), https://www.law360.com/articles/1516245/post-dobbs-hhs-guidance-brings-privacy-considerations [https://perma.cc/Y6KP-XM7A] ("For example, a state official in a state that bans abortion may issue a subpoena to a company using such tracking technologies seeking certain personal information relating to a consumer's online activity, including questions about birth control, pregnancy, pharmaceuticals or abortion services.").

[312] *See* Carter Gage, *The State Of Digital Health Care's Pandemic Transformation*, LAW360 (June 1, 2022, 6:08 PM), https://www.law360.com/articles/1498409/the-state-of-digital-health-care-s-pandemic-transformation [https://perma.cc/UV5P-RKRW]; Emily Olsen, *Digital health apps balloon to more than 350,000 available on the market, according to IQVIA report*, MOBIHEALTHNEWS (Aug. 4, 2021, 1:53 PM), https://www.mobihealthnews.com/news/digital-health-apps-balloon-more-350000-available-market-according-iqvia-report [https://perma.cc/9GFN-M895].

[313] Amina Kilpatrick, *Period tracker app Flo developing 'anonymous mode' to quell post-*Roe *privacy concerns*, NPR (June 30, 2022, 5:00 AM), https://www.npr.org/2022/06/30/1108814577/period-tracker-app-flo-privacy-roe-v-wade [https://perma.cc/JJE4-6DDE]; Nguyen & James, *supra* note 215.

[314] Nguyen & James, *supra* note 215; *see also* Torchinsky, *supra* note 189 (noting Flo and Clue as apps that can be used to track menstrual cycles).

pregnant, without making the practice clear to users.[315] The allegations stated that users' data had been shared with Facebook, Google, and other third parties that provided marketing and analytics services to the app.[316] Facebook software has been found to collect data "from many apps even if no Facebook account is used to log in and if the end user isn't a Facebook member."[317] Accordingly, "[t]he FTC alleged . . . that Flo promised to keep users' data private, when it actually disclosed data to third parties that provided marketing and analytics services to the app, including Facebook's analytics division as well as Alphabet Inc.'s Google analytics division and others."[318] A year before Flo's settlement, the developers of the app Glow had similarly settled with the California Attorney General over alleged

[315] *See* John D. McKinnon, *FTC Reaches Settlement with Flo Health over Fertility-Tracking App*, WALL ST. J., https://www.wsj.com/articles/ftc-reaches-settlement-with-flo-health-over-fertility-tracking-app-11610568915 [https://perma.cc/JL4P-88HJ] (last updated Jan. 14, 2021, 7:25 PM); Schechner & Secada, *supra* note 259; Torchinsky, *supra* note 189; Nguyen & James, *supra* note 215.

[316] McKinnon, *supra* note 315; Schechner & Secada, *supra* note 259 ("At the heart of the issue is an analytics tool Facebook offers developers, which allows them to see statistics about their users' activities—and to target those users with Facebook ads.").

[317] Schechner & Secada, *supra* note 259.

[318] McKinnon, *supra* note 315.

privacy and security violations relating to users' personal and health information.[319]

[81] These settlements may send a warning signal to developers of fertility apps or even health apps generally to protect and secure reproductive health care data.[320] Regardless, potentially incriminating data about those who have sought information about or received an abortion[321] will remain available for purchase until appropriate regulatory protections are in place. The next Section tackles this issue.

[319] *See* Press Release, Xavier Becerra, Att'y Gen., State Cal. Dep't of Just., Att'y Gen. Becerra Announces Landmark Settlement Against Glow, Inc. – Fertility App Risked Exposing Millions Of Women's Pers. & Med. Info. (Sept. 17, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93 [https://perma.cc/AH5L-ZFFR]; *see* Ariel Dobkin et al., *California Settles with Glow App Over Alleged Privacy and Security Violations*, JD SUPRA (Sept. 30, 2020), https://www.jdsupra.com/legalnews/california-settles-with-glow-app-over-85849/ [https://perma.cc/HY6Y-76YV]; *see also* Alex Pearce, *The California Attorney General's Settlement with Glow: A Wake-Up Call for Consumer Health App Developers*, JD SUPRA (Sept. 30, 2020), https://www.jdsupra.com/legalnews/the-california-attorney-general-s-71808/ [https://perma.cc/K6W6-6UGW] ("The settlement . . . imposes a rigorous set of injunctive terms on Glow that include some novel requirements designed to address the unique impacts that online privacy and data security lapses can have on women.").

[320] *See* Pearce, *supra* note 319.

[321] Press Release, Robert Bonta, Att'y Gen., State of Cal. Dep't Just., Att'y Gen. Bonta Emphasizes Health Apps' Legal Obligation to Protect Reprod. Health Info. (May 26, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-emphasizes-health-apps-legal-obligation-protect [https://perma.cc/LWG3-PS69] ("At a minimum, these apps should assess the risks associated with collecting and maintaining abortion-related information that could be leveraged against persons seeking to exercise their healthcare rights.").

IV. PROPOSAL FOR FEDERAL LEGISLATION: THE THREE CORNERS NEEDED TO PROTECT REPRODUCTIVE HEALTH CARE DATA PRIVACY

[82] Privacy's Fourth Amendment roots make for an awkward fit with digital data, and the legislative protections for health care data are inadequate. Because the law has failed to keep pace with technology, digital health care data, including reproductive health care data, is readily available to law enforcement, for free and increasingly for sale on the private market.

[83] Many have urged that comprehensive federal consumer data privacy legislation is needed to settle the pervasive issues around data regulation and consumer control of their own information.[322] Even if HIPAA is amended to resolve the problematic privacy exceptions and gaps that allow reproductive health care data to spread,[323] the digital breadcrumbs outside the HIPAA architecture will remain. Current data privacy laws are "a 'patchwork' of solutions to discrete privacy issues that leave significant gaps and open questions about which personal data are subject to protection

[322] *See, e.g.*, *U.S. Chamber of Commerce, others urge Congress to pass privacy legislation*, REUTERS (Jan. 13, 2022, 5:19 PM), https://www.reuters.com/world/us/us-chamber-commerce-others-urge-congress-pass-privacy-legislation-2022-01-13/ [https://perma.cc/ZR46-5EVQ]; Heather Deixler & Ty Kayam, *"Will You Share My Data, Please?" Evolving Legal Frameworks to Address Information Sharing by and for Patients*, AM. BAR ASS'N (June 23, 2021), https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2021/summer/will-you-share-my-data-please-evolving-legal-frameworks-address-information-sharing-and-patients/ [https://perma.cc/CR3D-LYRE]; Dellinger & Pell, *supra* note 7.

[323] *See supra* Part III.A.2.

and to what extent,"[324] as well as potentially conflicting compliance requirements.[325]

[84] Legislators have introduced at least eleven bills attempting to create a comprehensive federal data protection regime between 2018 and 2020,[326] with the most recent effort being the American Data Privacy and Protection Act (ADPPA) in 2022.[327] While the ADPPA did not pass in the 117th Congress, the bill provides a template for refining future federal privacy legislation.[328] Like the ADPPA, which "steer[ed] away from the [traditional U.S. consumer-focused] consent framework" of data privacy,[329] future legislation should follow a General Data Protection Regulation (GDPR)-like data protection regime instead, in which the default is that "personal information cannot be collected or processed unless there is a specific legal justification for doing so," based on the GDPR principle that "data

[324] Cason Schmit et al., *Data Privacy in the Time of Plague*, 21 YALE J. HEALTH POL'Y L. & ETHICS 152, 155 (2022).

[325] *See* Jason Oliveri, *Get Ready for a Comprehensive U.S. Data Privacy and Protection Law at the Federal Level...Maybe*, JD SUPRA (July 26, 2022), https://www.jdsupra.com/legalnews/get-ready-for-a-comprehensive-u-s-data-2555451/ [https://perma.cc/3XSQ-ZHML]; *see also* Lucy Porter & Brittney E. Justice, *Federal Privacy Legislation – Is it finally happening*?, NAT'L L. REV. (July 26, 2022), https://www.natlawreview.com/article/federal-privacy-legislation-it-finally-happening [https://perma.cc/G7NC-NXLJ] ("We now have five states—California, Connecticut, Colorado, Utah, and Virginia—that have enacted a comprehensive privacy law. There is mounting concern from key stakeholders of the impact that this 'patchwork' of laws will have on consumers and businesses.").

[326] *See* Schmit et al., *supra* note 324, at 171.

[327] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

[328] *H.R. 8152 (117th): American Data Privacy and Protection Act*, GOVTRACK, https://www.govtrack.us/congress/bills/117/hr8152 [https://perma.cc/6UK7-FKME] (last visited Oct. 15, 2023).

[329] *See* Porter & Justice, *supra* note 325.

protection is a fundamental human right . . . ."[330] Among the many aspects that such legislation should encompass are details on what is considered sensitive and personal information; standards for data minimization and retention; and a description of consumer rights, compliance, and enforcement.

[85] This Article's focus is solely on terms specific to reproductive health care data privacy post-*Roe*. To that end, this Article identifies "three corners" required for effective reproductive health care data privacy legislation: 1) define reproductive health care data as a separate category of protection; 2) implement a substantive prohibition against the sale of such reproductive health care data; and 3) provide the procedural protection of prohibiting admissibility of reproductive health care data without a warrant to criminalize an individual for seeking or obtaining an abortion.

[86] Importantly, these three corners should be part of a protective floor, rather than a ceiling that would preempt stronger state laws. States with and without privacy legislation could then build upon, rather than be limited by, this federal legislation in enacting state-level protections.[331]

A. First Corner: Carve Out a Specific Category for Reproductive Health Care Data

[87] To protect reproductive health care data privacy, the first corner of any effective legislation must be to define "reproductive health care" data. Such legislation must carve out a specific category of protection not only for health care data generally, but for reproductive health data specifically. An effective definition will recognize the many digital trails that can

[330] *See* Anupam Chander et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1747 (2021).

[331] *See* Schmit et al., *supra* note 324, at 174; India McKinney & Adam Schwartz, *EFF Urges Congress to Strengthen the American Data Privacy and Protection Act*, ELEC. FRONTIER FOUND. (June 14, 2022), https://www.eff.org/deeplinks/2022/06/eff-urges-congress-strengthen-american-data-privacy-and-protection-act [https://perma.cc/CRN4-BJER].

comprise health care data and secure reproductive health data's status as qualitatively distinct and sensitive among digital data, warranting specific privacy protection. Post-*Roe*, health care data's availability could allow law enforcement to target the patient and potentially charge her with serious crimes like feticide and homicide.[332] Meaningful privacy legislation should encompass not only the traditional health care records that HIPAA's exceptions and gaps leave unprotected, but also the digital trails that law enforcement can mine for free or purchase.[333] An inclusive definition of reproductive health care data within the classification of data to be considered private is thus the first corner of protection needed post-*Roe* within any comprehensive data privacy legislation.

[88] Legislation that distinguishes "reproductive health care data" within "sensitive covered data" as proposed by the ADPPA would recognize both the data's uniquely private nature and its heightened vulnerability. This definition should encompass text messages, direct messages, search history,

[332] *See* Dias, *supra* note 156.

[333] Pearce, supra note 319 (providing an example of legislation that addresses HIPAA's failure to protect data in apps with the Confidentiality of Medical Information Act (CMIA) which strengthens HIPAA's baseline requirements for regulatory compliance with health information by including "[c]onsumer health app developers"); *see* Bonta, *supra* note 321 ("Businesses that may need to comply with CMIA include health apps, such as some fertility trackers, and other types of pregnancy-related connected products that store details about a user's sexual activity, ovulation, and fertility test results. The CMIA requires businesses to preserve the confidentiality of medical information and prohibits the disclosure of medical information without proper authorization."); *see also* Maxine Henry, *California Confidentiality of Medical Information Act vs. HIPAA*, RISKOPTICS (Nov. 20, 2019), https://reciprocity.com/california-confidentiality-of-medical-information-act-vs-hipaa/ [https://perma.cc/CU8H-7D5Z].

geolocation data, and the data stored in fertility apps to criminalize an individual's reproductive health care choices.[334]

[89] While the draft ADPPA includes most of these forms of data within its definition of "sensitive covered data,"[335] it does not distinguish general health data from reproductive health care data specifically. However, language that recognizes data relating to health, sexual life, and sexual orientation already exists in state legislation and the European Union's data protection law.[336] Many states have legislated comprehensive privacy bills, including the California Consumer Privacy Act (CCPA), already considered one of the most expansive state statutes and superseded in 2023 by the California Privacy Rights Act (CPRA).[337] The CPRA, in addition to protecting "precise geolocation," expands upon the CCPA by including specific categories for "[p]ersonal information collected and analyzed concerning a consumer's health"; and "[p]ersonal information collected and

[334] *Supra* Part III.B; *see* Mike Lillis, *Pelosi outlines possible legislative response to* Roe *reversal*, THE HILL (June 27, 2022, 4:35 PM), https://thehill.com/homenews/house/3538652-pelosi-outlines-possible-legislative-response-to-roe-reversal/ [https://perma.cc/Q47N-LHJG] (noting House Speaker Nancy Pelosi's outline of a potential legislative response to Dobbs that prevents reproductive health data "such as that stored on apps" from being collected and distributed to third parties).

[335] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022) (defining "sensitive covered data" as "(ii) . . . [P]ast, present, or future physical health . . . or healthcare condition or treatment of an individual . . . (vi) Precise geolocation information . . . (vii) An individual's private communications such as voicemails, emails, texts, direct messages, or mail, or information identifying the parties to such communications . . . .").

[336] *Data protection under GDPR,* YOUR EUROPE (June 7, 2022), https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm [https://perma.cc/B7VB-SMEX].

[337] *Which States Have Consumer Data Privacy Laws?,* BLOOMBERG, https://pro.bloomberglaw.com/brief/state-privacy-legislation-tracker/ [https://perma.cc/G9E5-8F22] (last updated Sept. 7, 2023).

analyzed concerning a consumer's sex life or sexual orientation."[338] In April 2023, Washington State signed into law the My Health My Data Act (MHMD),[339] which focuses on information not covered under HIPAA, including "reproductive or sexual health information."[340]

[90] Delineating categories of protection for data relating to health, sexual life, and sexual orientation is one way the CPRA and MHMD more closely resembles the European Union's General Data Protection Regulation (GDPR). [341] The GDPR provides that processing "special categories of personal data," including "data concerning health *or* data concerning a natural person's sex life or sexual orientation shall be prohibited."[342] Federal privacy legislation likewise should expand upon existing language in state statutes and the example of the GDPR to explicitly protect reproductive health care data.

[91] Federal legislation must also protect location information related to reproductive healthcare. The My Body, My Data Act of 2022, introduced

[338] *See* CAL. CIV. CODE, §§ 1798.140 (ae)(1)(C), (ae)(2)(B)–(C) (Deering 2018)*; see also* Jason C. Gavejian et al., *California Consumer Privacy Act, California Privacy Rights Act FAQs for Covered Businesses*, JACKSON LEWIS (Jan. 19, 2022), https://www.jacksonlewis.com/publication/california-consumer-privacy-act-california-privacy-rights-act-faqs-covered-businesses [https://perma.cc/V2DA-W394].

[339] WASH. REV. CODE §19.373.005 (2023).

[340] Mike Hintze, *The Scope of "Consumer Health Data"*, HINTZE LAW (Apr. 12, 2023), https://hintzelaw.com/hintzelaw-blog/2023/4/12/wa-my-health-my-data-act-pt-2-scope-of-consumer-health-data?rq=washington [https://perma.cc/QPW6-8W2Y].

[341] *See generally* Christina Whiting, *Tevora Data Privacy Law Comparison: CCPA, CPRA, GDPR, and PIPEDA*, TEVORA (Mar. 4, 2021), https://www.tevora.com/blog/tevora-data-privacy-law-comparison-ccpa-cpra-gdpr-and-pipeda/ [https://perma.cc/49PX-E9CQ] (stating, "CPRA makes major strides in closing the gap with GDPR. While there are provisions in GDPR that don't exist in CPRA—and visa verse [sic]—The [sic] California and European laws now have a lot in common.").

[342] 2018 O.J. (L 127) 23.5.2018 (emphasis added).

by Representative Sara Jacobs, Senator Ron Wyden, and Senator Mazie Hirono, recognizes the need to create various privacy protections specifically for reproductive health care data and that location data must be included within that definition.[343] The bill defines "personal reproductive or sexual health information" to mean "personal information relating to the past, present, or future reproductive or sexual health of an individual," and specifically includes "efforts to research or obtain reproductive or sexual information services or supplies, including *location information* that might indicate an attempt to acquire or receive such information services or supplies."[344] Although the bill did not receive a vote in the 2022 term and therefore was not enacted,[345] it provides an example of legislation that would protect personal reproductive health care data specifically, and recognizes that location information is intrinsically linked to reproductive health care data.[346]

[92] Moreover, reproductive health care data's privacy protections should not depend upon a timeline. The My Body, My Data Act explicitly includes personal information relating to the "past, present, or future" health

[343] My Body, My Data Act, H.R. 8111, 117th Cong. (2022); *see also* Press Release, Ron Wyden, U.S. Senator, Wyden, Colleagues Introduce My Body, My Data Act to Protect Reproductive Health Data (June 21, 2022), https://www.wyden.senate.gov/news/press-releases/wyden-colleagues-introduce-my-body-my-data-act-to-protect-reproductive-health-data [https://perma.cc/W328-KYPT].

[344] H.R. 8111 § 6(6), (6)(A) (emphasis added).

[345] *H.R. 8111 (117th): My Body, My Data Act of 2022,* GOVTRACK (July 20, 2022), https://www.govtrack.us/congress/bills/117/hr8111/summary [https://perma.cc/Y9G3-GX7U].

[346] *See* My Body, My Data Act, H.R. 8111, 117th Cong. (2022); *see also* Wyden Press Release, *supra* note 343 ("The *My Body, My Data Act* is the first Congressional action to strengthen digital privacy and protect personal reproductive health information specifically. The bill would create a new national standard to protect personal reproductive health data, enforced by the Federal Trade Commission (FTC). By minimizing the personal reproductive health data that is collected and retained, the bill would prevent this information from being disclosed or misused.").

of an individual in its definitions of "personal reproductive or sexual health information."[347] In doing so, the bill recognizes that traditional medical records have included documentation of past conditions, present medical treatment, or future possible treatment. Digitally-generated reproductive health care data, likewise, should include past, present, and anticipated conditions and treatment, and all categories deserve protection since law enforcement's purpose may be to criminalize an individual's past, present, or anticipated reproductive health care choice.

[93] Reproductive health care data likewise deserves protection independent of any physical location. The private nature of the data should remain unaffected by whether the data is saved locally on a device, a server, or the cloud, and regardless of where the device or server may be located at any particular given point. Unlike physical objects, "[d]ata . . . is not tied to territory."[348] Federal privacy legislation would overcome the current jurisdictional divide in which some states seek to criminalize women who obtain abortions, either when they return to their home voluntarily or even potentially through extradition.[349] As the dissenting justices predicted in *Dobbs*, "[a]fter this decision, some States may block women from traveling out of State to obtain abortions, or even from receiving abortion medications from out of State."[350] States like Texas and Oklahoma have enacted

[347] My Body, My Data Act, H.R. 8111, 117th Cong. (2022).

[348] Park, *supra* 43, at 18–19 (2019) (quoting Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 554 (2017)).

[349] *See, e.g.*, Erin Coulehan, *Abortion "Bounty" Laws in States Like Texas and Oklahoma: How They Work*, TEEN VOGUE (July 7, 2022), https://www.teenvogue.com/story/abortion-bounty-laws [https://perma.cc/EE33-GTMY] ("This past legislative session, some Missouri legislators were even attempting to prevent people from traveling out of state to seek abortion care[,] . . . [while the] New Mexico governor . . . issued an executive order 'securing access to reproductive health care services' and declaring the state 'will not entertain extradition attempts from other states relating to receiving or performing reproductive services.'").

[350] Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2318 (2022) (Breyer, Sotomayor, and Kagan, JJ., dissenting).

"bounty-style laws" that deputize private citizens by granting them the authority to enforce anti-abortion laws in exchange for cash.[351] Such efforts to restrict interstate travel for purposes of abortion care would be undercut by federal legislation that includes reproductive health care data in its definition of sensitive covered data regardless of where the data is saved, where the device or server is located, or any other measures that purport to tie digital data to a physical space in order to assert jurisdiction over it. Uniform protection would preserve the essence of the right to privacy the Supreme Court recognized in *United States v. Katz*: that "the Fourth Amendment protects people, not places."[352] "The concept of protecting people, not places, has never been more fitting than now, where 'places' may very well be cyberspaces."[353]

[94] Carving out a specific category of privacy protection for reproductive health care data that includes these forms of data within its mantle would ensure that the data falls within the tailored protections of the other two corners of reproductive health care data. This second corner is discussed next.

B. Second Corner: Prohibit Data Brokers from Selling Reproductive Health Care Data

[95] Reproductive health care data, once inclusively defined as a unique category of sensitive covered data, needs to be protected with substantive

[351] *See* Coulehan, *supra* note 349 ("A proposed [Missouri] amendment tacked on to an antiabortion bill criminalizing the procedure would have permitted private citizens to bring civil litigation against anyone who helps a Missouri resident have an abortion, including those who don't reside in the state.").

[352] Katz v. United States, 389 U.S. 347, 351 (1967).

[353] Portions of this paragraph adapted from Park, *supra* note 43, at 19 ("*Katz* presciently recognized that 'the Fourth Amendment protects people, not places' in striving to meet its underlying purpose of curbing excessive governmental power. ").

prohibitions.[354] As described below, current privacy practices intended to insulate data or provide consumers with redress are inadequate. Legislation must instead hone in on the specific activity that threatens reproductive health care data privacy. Thus, the second corner of the legislation must prohibit the sale of reproductive health care data to law enforcement, with an expanded definition of "sale," in contrast to the common, but ineffective, security practices of requiring notice and consent, data anonymization, or registration.

[96] First, the notion that requiring notice and consent protects the individual is illusory on multiple fronts. In theory, clicking "I agree" to a website's terms of service and privacy policy means that the company has provided notice that the site will collect and process the individual's personal data, and that the individual has consented to it.[355] However, the "long and complex privacy notices" are "written by lawyers for lawyers . . . ."[356] Even if the notices were concise and comprehensible, the sheer frequency with which individuals are presented with such language precludes the ability to carefully consider them all. Finally, notice and consent offers no meaningful choice, since declining means abandoning the service—an unrealistic option in a society where basic activities like

[354] *See* Lina M. Khan, Chair, Fed. Trade Comm'n, Remarks at International Association of Privacy Professionals' Global Privacy Summit 6 (Apr. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf [https://perma.cc/AV77-CJSZ] (urging that privacy protections include substantive as well as procedural protections).

[355] *See* Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, NEW AMERICA (Mar. 23, 2020), https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/ [https://perma.cc/XB8J-7T7A]; *see also* Fred H. Cate & Viktor Mayer-Schönberger, *Notice and Consent in a World of Big Data*, 3 INT'L DATA PRIV. L. 67, 67 (2013).

[356] Cate & Mayer-Schönberger, *supra* note 355.

making purchases, scheduling appointments, checking one's bank account, and receiving delivery date updates increasingly require going online.[357]

[97] The common practice of aggregating or anonymizing data does not provide the privacy to that data that companies claim.[358] While the HHS, for example, provides detailed guidance on methods for de-identifying protected health information in accordance with HIPAA,[359] reidentifying an individual from a supposedly anonymized data set "is disturbingly easy, even when one is working with an incomplete data set."[360] Technology companies could likely triangulate anonymized information with existing user information to reidentify the patient, then sell that data to a third party.[361] A research team from the University of Melbourne, for example, discovered how simple it was to learn about an individual's "entire medical history without their consent" by comparing de-identified information to

[357] *Cf.* Park, *supra* note 43, at 20 (questioning whether consumer awareness of cell-site location information necessarily leads to a meaningful choice about whether to assent to use of that technology).

[358] Sophie Bushwick, *"Anonymous" Data Won't Protect Your Identity,* SCI. AM. (July 23, 2019), https://www.scientificamerican.com/article/anonymous-data-wont-protect-your-identity/ [https://perma.cc/TBX4-Q2R4].

[359] Off. for Civ. Rts., *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html [https://perma.cc/QP5L-RWBX] (last updated Oct. 25, 2022).

[360] Bushwick, *supra* note 358; *see* Stacey A. Tovino, *Not So Private*, 71 DUKE L.J. 985, 990–91 (2022) ("[P]urportedly de-identified data can—and increasingly will—be reidentified.").

[361] Bindley, *supra* note 163.

other publicly available information.[362] The FTC has warned companies not to "try to placate consumers' privacy concerns by claiming they anonymize or aggregate data," stating such claims may constitute deceptive trade practices in violation of the FTC Act.[363] The FTC was particularly concerned about the ease with which location data, which this Article urges should be included under reproductive health data's umbrella, can be deanonymized.[364]

[98] The tactic of requiring data brokers to register with the state is also inadequate. In California, for example, data brokers are required to register with the Attorney General on its internet website that is accessible to the public.[365] Vermont also requires an annual registration.[366] While such registries do make available to the public a list of data brokers, they fail to "put any meaningful controls on companies selling, licensing or otherwise

[362] Olivia Solon, '*Data is a fingerprint': why you aren't as anonymous as you think online*, THE GUARDIAN (July 13, 2018, 4:00 AM), https://www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy [https://perma.cc/VMG3-3V7Z].

[363] Cohen, *supra* note 183.

[364] *Id.* (noting that "Significant research has shown that 'anonymized' data can often be re-identified, especially in the context of location data. One set of researchers demonstrated that, in some instances, it was possible to uniquely identify 95% of a dataset of 1.5 million individuals using four location points with timestamps. Companies that make false claims about anonymization can expect to hear from the FTC.").

[365] CAL. CIV. CODE § 1798.99.80 (Deering 2020).

[366] VT. STAT. ANN. tit. 9, § 2446 (2017).

sharing Americans' sensitive data on the open market."[367] The strategy provides information but no substantive curb on broker practices. Moreover, such registry-focused laws replicate the problem with notice and consent requirements: They "place the burden entirely on consumers, who may have to file opt-out requests with hundreds if not thousands of companies."[368] Even that tremendous effort may not be enough; under some proposed laws, brokers may "continue selling information on those individuals anyway—claiming, for example, that said information is not explicitly tied to a name."[369]

[99] Future legislation must implement substantive controls on the sale of private reproductive health care data to law enforcement. This means expressly prohibiting the sale to law enforcement of the ample digital breadcrumbs discussed above that can be obtained free or by purchase, including text messages, direct messages, search history, and geolocation data, as well as conventional health care data.

[367] Justin Sherman, *Examining State Bills on Data Brokers*, LAWFARE BLOG (May 31, 2022, 8:01 AM), https://www.lawfaremedia.org/article/examining-state-bills-data-brokers [https://perma.cc/YT29-EX7W] (discussing state bills: "For example, the Delaware law broadens the scope of a data broker (data market participant) definition beyond the California and Vermont laws, but it still orients its regulation on setting up a state website that lists data brokers, instead of implementing controls on data selling. The same goes for California's bill, which would have broadened the scope of the legal term 'data brokers' but would not have stopped a data broker from selling a minor's GPS location or licensing data on women's health conditions to a business in another state. Given the documented harms of the data brokerage ecosystem—from enabling and exacerbating gender violence to advertising data on military personnel and exposing the U.S. to national security risks—these notification- and consent-oriented approaches are wholly insufficient to protect individuals and society from ongoing harm.").

[368] *Id.*

[369] *Id.*

[100] Senator Elizabeth Warren proposed prohibiting data brokers from transferring and selling certain sensitive data in a June 2022 bill.[370] The Health and Location Data Privacy Act of 2022 recognizes the need to regulate data brokers, and defines health data to include location data.[371] The bill's definition of "health data" includes "any past, present, or future . . . health condition of an individual" such as "pregnancy and miscarriage."[372]

[101] Similarly, in 2021, The Fourth Amendment Is Not For Sale Act[373] proposed barring law enforcement from purchasing consumer communications or location information from data brokers.[374] One of the bill's co-sponsors, Senator Mike Lee of Utah, explained, "[t]he federal government should not be allowed to skirt the Fourth Amendment's existing warrant requirements and surveillance laws by purchasing Americans' data from third-party brokers. This legislation will protect the civil liberties of Americans by closing loopholes in existing law."[375]

---

[370] Health and Location Data Protection Act of 2022, S. 4408, 117th Cong.; *see* Alder, *Bill Seeks to Ban Data Brokers*, *supra* note 15.

[371] *See generally* Health and Location Data Protection Act of 2022 (stating that its purpose is "[t]o prohibit data brokers from selling and transferring certain sensitive data.").

[372] *Id.* at § 4(4)(B) ("The term 'health data' means data that reveal or describe . . . any past, present, or future disability, physical health condition, mental health condition, or health condition of an individual, including, but not limited to, pregnancy and miscarriage.").

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

[374] *Id.*; *see* LINEBAUGH, *supra* note 196.

[375] Press Release, Ron Wyden, U.S. Senator, Wyden, Paul and Bipartisan Members of Congress Introduce the Fourth Amendment is Not for Sale Act (Apr. 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act- [https://perma.cc/PV8T-EC36].

[102] Finally, the definition of "selling" to data brokers must also be broad enough to include licensing and other forms of sharing data. Otherwise, the term "selling" may inadvertently exclude activity that may not be captured under a strict definition, such as real-time bidding.[376] The Health and Location Data Protection Act bill anticipates this by expansively providing that "[i]t shall be unlawful for a data broker to sell, resell, license, trade, transfer, share or otherwise provide or make available" an individual's private data.[377]

[103] Although the Warren bill did not pass in 2022, it—along with the My Body, My Data Act, the Fourth Amendment Is Not For Sale Act, and state legislation such as the CPRA—provides a blueprint for future legislation that adds a necessary substantive prohibition against the selling of protected reproductive health data by data brokers to law enforcement.

C. Third Corner: Bar Admissibility of Reproductive Health Care Data Obtained Without a Warrant

[104] Not only must data brokers be prohibited from selling reproductive health care data, but federal legislation must specifically bar law enforcement from using data that would not have been obtainable without a warrant as the basis for a post-*Roe* prosecution. This third corner adds a necessary procedural layer to protections for private reproductive health care data.

---

[376] *See* Sherman, *supra* note 367 (noting that California SB-1059 has proposed "amend[ing] the definition of a data broker so that it includes not just the selling of data but the sharing of data," although critiquing a "focus on the outright selling of data," because, "[f]or example, many companies share their own users' data with real-time bidding networks for online ads, an action that sends individuals' sensitive information (from income level to GPS location) to third parties but that may not be captured under the strict definition of 'selling' individuals' information."); *see also* Doughty & Sircar, *supra* note 294 (re: auction-style real-time bidding).

[377] Health and Location Data Protection Act of 2022, S. 4408, 117th Cong. § 2(a) (2022).

[105] A search warrant requires probable cause that evidence of crime will be found.[378] Even when the suspected monitored activity is clearly illegal, evidence seized without a valid warrant is unconstitutional and therefore inadmissible.[379] For example, in *Carpenter v. United States*'s armed robbery investigation, the Court held that identifying the defendant based on cell-site location information obtained without a warrant was unconstitutional.[380] Likewise, in *United States v. Jones*'s drug possession investigation, the Court held that attaching a GPS tracker to monitor a defendant's movements on public streets without a warrant was unconstitutional.[381] Unlike armed robbery or illegal drug possession, which are uniformly illegal, abortion faces a panoply of drastically contradictory state criminal laws. Abortion uniquely presents potentialities ranging from being completely legal up to and including being convicted of homicide, based on one's health data.[382] As noted above, however, HIPAA's exceptions under which law enforcement can obtain health data by warrant center around public or patient safety, not criminal prosecution of the

[378] Barry Friedman & Orin Kerr, *The Fourth Amendment*, NAT'L CONST. CTR., https://constitutioncenter.org/the-constitution/amendments/amendment-iv/interpretations/121 [https://perma.cc/9S6Z-QH22] (last visited Oct. 15, 2023).

[379] *Id.*

[380] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

[381] United States v. Jones, 565 U.S. 400, 431 (2012).

[382] *See Why Laws Are Different State to State*, WIDERMAN MALEK (Feb. 11, 2016), https://www.legalteamusa.net/different-state-different-law/ [https://perma.cc/BH9X-G6GN] (noting other areas exist where criminal liability can vary, but prosecution is not based on the individual's health data. Examples include gun control, child custody, trucking and motor carriers, and businesses and corporations); *see also* Emma Kaufman, *Territoriality in American Criminal Law*, 121 MICH. L. REV. 353, 362–63 (2022) (explaining that American criminal law arises from the crimes connected to a particular place because each state has its own criminal code); *see, e.g.*, Michelle Rindels, *Indy Explains: How legal prostitution works in Nevada*, NEV. INDEP. (May 27, 2018, 2:10 AM), https://thenevadaindependent.com/article/the-indy-explains-how-legal-prostitution-works-in-nevada [https://perma.cc/7FD2-QUYP] (providing an example where prostitution is legal only in one state, Nevada).

patient.[383] A bright-line warrant requirement is thus consistent with HIPAA's purpose of protecting the patient. Such a requirement is also consistent with the HHS' 2022 guidance memo relating to reproductive health care, stating that "[t]he Privacy Rule permits but *does not require* covered entities to disclose PHI about an individual for law enforcement purposes" such as "a court order or court-ordered warrant, or a subpoena or summons . . . ."[384]

[106] The "murky distinction between abortions and miscarriages" further complicates the potential abuse of personal data.[385] Discrepancies also lie in the ability to travel to obtain an abortion.[386] Such contradictory or unclear laws can lead to drastically disparate treatment of an individual based on the same reproductive health care data.

[107] Lack of legal clarity will contribute to the incidence of criminalization. Even before *Dobbs*, prosecuting pregnancy loss had become more common. The National Advocates for Pregnant Women, a nonprofit advocacy organization, found that the number of cases where pregnancy loss was used in a criminal prosecution or investigation almost quadrupled from 2006–2020, in comparison to the period after *Roe* was decided in 1973 until 2005.[387] States are now targeting pregnant people under "fetal harm" laws originally intended to deter violence against pregnant people but increasingly being used "to investigate and prosecute different forms of pregnancy loss, including miscarriages, stillbirths and

[383] *See supra* Part III.A.

[384] Off. for Civ. Rts., *supra* note 134 (emphasis in original).

[385] Boodman et al., *supra* note 130.

[386] *See supra* Part III.B.

[387] Robert Baldwin III, *Losing a pregnancy could land you in jail in post*-Roe *America*, NPR (July 3, 2022, 5:27 AM), https://www.npr.org/2022/07/03/1109015302/abortion-prosecuting-pregnancy-loss [https://perma.cc/MV36-NJLY].

self-induced abortions."[388] Individuals have been "investigated, detained or arrested . . . for miscarrying after otherwise noncriminal acts, such as attempting suicide, falling down a flight of stairs and drinking alcohol."[389] Such policing over the lives of pregnant people can be expected to increase.[390]

[108] Even the Network Advertising Initiative (NAI), an industry trade group founded in 2000 that develops self-regulatory standards for online advertising, discourages sensitive data disclosure "except as necessary to comply with a valid legal obligation."[391] The NAI published Precise Location Information Solution Provider Voluntary Enhanced Standards (Enhanced Standards) in June 2022.[392] Notably, the Enhanced Standards specifically prohibit disclosing data relating to "[m]edical facilities that cater predominantly to sensitive conditions, such as . . . fertility or abortion clinics[.]"[393] The Enhanced Standards also limits disclosing "Precise

[388] *Id.*; *see supra* Part III.B.1.a.

[389] Aliyah Tihani Salim & Shivana Jorawar, *Roe is over. Prison sentences are on the way*., NBC NEWS THINK (July 3, 2022, 5:40 AM), https://www.nbcnews.com/think/opinion/abortion-laws-punishing-women-supreme-court-ended-roe-rcna36268 [https://perma.cc/Z3HG-AZKT].

[390] *See id.*; Baldwin, *supra* note 387 (stating that "legal experts expect that prosecutions may continue to increase").

[391] *See About the NAI*, NAI, https://thenai.org/about/ (last visited Oct. 9, 2023); *see also NAI Precise Location Information Solution Provider Voluntary Enhanced Standards*, NAI (June 22, 2022), https://thenai.org/accountability/precise-location-information-solution-provider-voluntary-enhanced-standards/ [https://perma.cc/PM6B-DPJ8] [hereinafter *NAI Enhanced Standards*].

[392] *NAI Enhanced Standards*, *supra* note 391, at 3 (identifying location data brokers Cuebiq, Foursquare, and Precisely PlaceIQ as having voluntarily adopted the Enhanced Standards).

[393] *Id.* at 2 (providing that companies "shall not use, allow the use of, sell, or share any information about device or user activity correlated to a known Sensitive [Point of Interest].").

Location Information for law enforcement . . . or bounty-hunting purposes, except as necessary to comply with a valid legal obligation."[394] In response to the continued emergence of state privacy laws, however, the NAI temporarily paused enforcement of its self-regulatory code on July 1, 2023 in an effort to maintain alignment with those laws.[395]

[109] The "third corner" warrant requirement for reproductive health data should encompass all the mechanisms through which law enforcement can obtain identifiable data without probable cause: subpoena or order; law enforcement surveillance technology; and general data collection. This approach ensures that all methods, traditional and otherwise, are Fourth Amendment searches when the data is sought to criminalize abortion or related services, including keyword and geofence reverse warrants.[396] Since *United States v. Chatrie* left unresolved the issue of whether a geofence warrant should classify as a search,[397] settling the matter with legislation "could not only protect the privacy of citizens, but also could relieve

[394] *Id.* at 3; *see* Practical Law Commercial Transactions, *NAI Publishes Enhanced Standards on Tracking Sensitive Location Data*, THOMSON REUTERS (June 28, 2022), https://content.next.westlaw.com/w-036-0877?elq_mid=35967&elq_cid=18914657&elq_ename=L_PL_NSL_NA_PLIPT76_US_em1_20220706&cid=9002340&email=euparkesq%40gmail.com&sfdccampaignid=7011B000001xTee&chl=Em&utm_medium=email&utm_source=eloqua&utm_campaign=L_PL_NSL_NA_PLIPT76_US_20220706&utm_content=9002340&isplcus=true&transitionType=Default&contextData=%28sc.Default%29 [https://perma.cc/BK8F-AUNZ] ("The Enhanced Standards are in addition to the existing disclosure and consent requirements under the NAI Code of Conduct and apply to companies that voluntarily commit to following them.").

[395] *Code of Conduct*, NAI, https://thenai.org/accountability/code-of-conduct/ [https://perma.cc/83AZ-326B] (last visited Oct. 9, 2023).

[396] *See supra* Part III.B.1.

[397] United States v. Chatrie, 590 F. Supp. 3d 901, 932 (E.D. Va. 2022); *see supra* Part III.B.1.b.

companies of the burden to police law enforcement requests for the data they lawfully have."[398]

[110] Effective privacy legislation must also include a specific and consistent procedural boundary for how potential crimes associated with abortion are prosecuted. Given that reproductive health care choice does not share baseline recognition as a crime consistently across jurisdictions, the boundary should be that no state can use reproductive health care data that was obtained without a warrant as evidence to prosecute an individual—a standard that is no greater and no less than the Fourth Amendment requires. Alone, the warrant requirement cannot adequately protect reproductive health care choices from criminalization.[399] Together, however, the three corners would formalize common-sense boundaries that the HHS, the NAI, and federal bills have already envisioned.

V. CONCLUSION

[111] In December 2022, President Biden signed the Respect for Marriage Act into law mandating federal recognition for same-sex and interracial marriages.[400] Along with the marriage protection bill, the House of Representatives passed a bill in July 2022 to protect access to

[398] Orin Kerr, *The Fourth Amendment and Geofence Warrants: A Critical Look at* United States v. Chatrie, LAWFARE (Mar. 12, 2022, 3:34 PM), https://www.lawfareblog.com/fourth-amendment-and-geofence-warrants-critical-look-united-states-v-chatrie [https://perma.cc/JLK6-UVAS] ("This case has arisen because no extant legislation prevents Google or its competitors from collecting and using this vast amount of data.").

[399] *See* Part II.B.1.; *see also, e.g.*, Dellinger & Pell, *supra* note 7.

[400] Respect for Marriage Act, H.R. 8404, 117th Cong. (2022).

contraception[401] from potential Supreme Court intervention,[402] but the contraception bill faced resistance from the Senate.[403] Legislation codifying the right to abortion similarly faces a barrier with the Senate; although the U.S. House in the 117th Congress voted twice to pass the Women's Health Protection Act (WHPA), both times the bill failed to find enough votes in the Senate to overcome filibuster.[404] The WHPA was introduced again in the House in March 2023.[405] On the other hand, the draft ADPPA demonstrates that digital data privacy, at least, is a bipartisan concern.[406]

[112] Some companies have attempted to support employees by offering to cover travel costs to a state where abortion is legal.[407] These well-

[401] Right to Contraception Act, H.R. 8373, 117th Cong. (2022).

[402] Sahil Kapur, *House passes legislation to enshrine a right to contraception in federal law*, NBC NEWS, https://www.nbcnews.com/politics/congress/house-passes-legislation-enshrine-right-contraception-federal-law-rcna39167 [https://perma.cc/A4HS-DJWU] (last updated July 21, 2022, 12:41 PM).

[403] Cassidy Morrison, *Democratic contraception bill faces Senate trouble over religious freedom*, WASH. EXAM'R (July 22, 2022, 1:54 PM), https://www.washingtonexaminer.com/restoring-america/community-family/birth-control-bill-faces-uphill-in-senate [https://perma.cc/4QNL-QALG].

[404] *Women's Health Protection Act (WHPA)*, CTR. FOR REPROD. RTS. (June 23, 2023), https://reproductiverights.org/the-womens-health-protection-act-federal-legislation-to-protect-the-right-to-access-abortion-care/ [https://perma.cc/RRT3-3T6M]; *U.S. Senate Fails to Pass Abortion Rights Legislation*, CTR. FOR REPROD. RTS. (May 11, 2022), https://reproductiverights.org/us-senate-fails-to-pass-abortion-rights-bill/ [https://perma.cc/EB7L-5QEN].

[405] *Women's Health Protection Act (WHPA)*, *supra* note 404.

[406] *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

[407] Chris Marr & Robert Iafolla, *Can States Ban Employer Abortion Aid? Post-*Roe *Limits Explained*, BLOOMBERG LAW (June 28, 2022, 10:17 AM), https://news.bloomberglaw.com/daily-labor-report/can-states-ban-employer-abortion-aid-post-roe-limits-explained?utm_source=twitter&campaign=3F84A786-F719-11EC-BF02-960750017A06&utm_medium=lawdesk [https://perma.cc/EB7L-5QEN].

intentioned offers may give rise to a new set of privacy issues.[408] Employees who wish to take advantage of these policies would have to disclose information that they may have wished to keep private from their employers, namely that they are pregnant, to access reproductive health care.[409] Moreover, the employers may find themselves threatened by state attorneys general that "seek to hold the companies liable as aiding and abetting violations of state abortion prohibitions."[410]

[113] In May 2023, the Supreme Court upheld a California law on humane treatment of pigs, finding that the pork producer failed to demonstrate a substantial burden on interstate commerce.[411] The case had been closely watched for its potential impact on states' ability to regulate conduct outside their borders, including the ability of a state to forbid its citizen from traveling and receiving a legal abortion.[412] While the decision seems to allay that concern, in another pending case the judge has asked the parties to address whether the Supreme Court's ruling supports, or argues against, the

[408] Katie Reilly, *New Corporate Policies on Abortion Travel Spark Worries About Employees' Privacy*, TIME, https://time.com/6192361/companies-abortion-travel-paying-privacy/ [https://perma.cc/65PB-QZFA] (last updated June 30, 2022, 11:07 AM).

[409] *See id.*

[410] *See* Ann M. O'Leary et al., *SCOTUS Overrules* Roe v. Wade*: Part I: Potentially Wide-Ranging Impact on Companies Navigating Employee Benefits, Privacy Protections, and Law Enforcement Demands*, JENNER & BLOCK (June 27, 2022), https://www.jenner.com/a/web/27axGaoqNhTWZpA7wR4XW2/4k1Xmi/SCOTUS_Overrules_Roe_Wade_Part_I.pdf. [https://perma.cc/XV23-3UAQ]; *see* Marr & Iafolla, *supra* note 407.

[411] Nat'l Pork Producers Council v. Ross, 143 S. Ct. 1142, 1162–63 (2023).

[412] Ann M. O'Leary et al., *SCOTUS Overrules* Roe v. Wade*: Part II: Outlining the Threat to Reproductive Rights Across the United States,* JENNER & BLOCK (June 27, 2022), https://www.jenner.com/a/web/iUusLf2p5TVmLKXnE4USWC/4k1Z5M/scotus_overrules_roe_wade_part_ii.pdf [https://perma.cc/F6V7-ZHJG].

drug manufacturer's claim that West Virginia's ban of mifepristone violates the Commerce Clause.[413]

[114] In the face of ongoing uncertainties, federal privacy legislation provides the most promising means for reproductive health care data protection. Passing such legislation will not be easy, since anti-abortion states will resist privacy protections that limit the ability to criminalize reproductive health care choices. In the meantime, the Supreme Court majority's "pinched view" of the Constitution as "historically circumscribed," rather than "responsive to new societal understandings and conditions,"[414] implicates abortion and constitutional protections generally. The greatest risks fall on marginalized populations with rights recognized in landmark Supreme Court cases that may be subject to renewed scrutiny under a narrowed view of the right to privacy. Likewise, *Dobbs* will disparately impact not just women but low-income women of color subject to disproportionate targeting on matters related to pregnancy, with detrimental consequences to both their health and freedom.[415]

[115] As Offred said in *The Handmaid's Tale*, "[n]othing changes instantaneously: in a gradually heating bathtub, you'd be boiled to death before you knew it."[416] Unless we want to find ourselves boiling to death, we must enact federal legislation protecting our privacy, and specifically reproductive health care data privacy, now.

---

[413] Mary Anne Pazanowski, *Top Court's Pork-Producer Ruling Could Affect Abortion-Pill Suit*, BLOOMBERG LAW (May 22, 2023, 3:01 PM), https://news.bloomberglaw.com/health-law-and-business/genbiopro-west-virginia-address-top-court-commerce-clause-case [https://perma.cc/57D4-KRHV].

[414] Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2325–26 (2022) (Kagan, J., dissenting).

[415] *See supra* Part I.

[416] ATWOOD, *supra* note 1, at 56.