PREGNANCY PANOPTICON

Abortion Surveillance After *Roe*

ALBERT FOX CAHN, ESQ.
ELENI MANIS, PHD, MPA

MAY 24, 2022

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

Supported in part by a grant from the Open Society Foundations and by the John D. and Catherine T. MacArthur Foundation

I. Introduction

Abortion rights will soon be a thing of the past for millions of Americans. At the time of publication, a leaked Supreme Court draft opinion shows a majority of justices are poised to strike down *Roe v. Wade*, *Planned Parenthood v. Casey*, and any federal constitutional right to abortion. But repealing a half century of reproductive rights won't transport Americans back to 1973, it will take us to a far darker future, one where antiquated abortion laws are enforced with cutting edge technology. Sweeping abortion laws are already on the books in many states, primed to go into effect the moment the Supreme Court's decision is published. But those sprawling bans won't enforce themselves. Police, prosecutors, and private anti-abortion litigants will weaponize existing American surveillance infrastructure to target pregnant people and use their health data against them in a court of law. This isn't speculation—it's already happening.

Abortion opponents surveil pregnant people and abortion providers to chill their reproductive freedoms.[1] Hospitals track pregnant patients with suspicionless drug testing,[2] while police harness surveillance to enforce existing abortion laws. Nearly every aspect of pregnant peoples' online lives is already targeted—including search histories, online purchases, and messages—while cellphone location data is used to track their movements in physical space.[3] If this is the state of surveillance today, in an America with abortion rights, what surveillance will we see in a post-*Roe* future?

Lawmakers will likely pressure police and prosecutors to use all of the tracking tools they have to target health providers, pregnant people, and anyone helping them to access care. And with all mass surveillance, there will be countless bystanders targeted, too, those who will be jailed because of miscarriages, ectopic pregnancies, and inaccurate data. This is a bleak forecast for the future, but

[1] Alice Clapman, "Privacy Rights and Abortion Outing: A Proposal for Using Common-Law Torts to Protect Abortion Patients and Staff," *The Yale Law Journal* 112, no. 6 (2003): 1545–76, https://doi.org/10.2307/3657452.
[2] Grace Howard, "The Pregnancy Police: Surveillance, Regulation, and Control," *Harvard Law and Policy Review* 14, no. 2 (2019), https://harvardlpr.com/wp-content/uploads/sites/20/2020/11/Howard.pdf.
[3] Sharona Coutts, "Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits - Rewire News Group," *Rewire News Group*, May 25, 2016, https://rewirenewsgroup.com/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/.

there are still steps that providers, lawmakers, and members of the public can take to protect pregnant people from this looming surveillance state, if only we act now.

II. Current Analog Surveillance of Pregnant People

For 49 years, *Roe v. Wade* and *Planned Parenthood v. Casey* promised pregnant people significant reproductive autonomy. Although states dramatically expanded abortion access restrictions in the decades since *Roe* was decided, its core holding—granting pregnant people the right to determine whether to seek abortion prior to viability—remained a key pillar of American constitutional law. However, abortion rights have often been far more limited in practice than they appear on paper. Non-state actors use surveillance as one of many tactics to harass pregnant people and providers, chilling their exercise of reproductive rights. Activists film and publicly identify abortion seekers and medical staff.[4] They map patients' social networks and contact their families, leading to familial coercion and even violence.[5] They track the license plates of people entering clinics.[6] One anti-abortion advocate even created a website listing the names, addresses, phone numbers, and photographs of reproductive healthcare providers…labeling each doctor as "working," "wounded," or "fatality."[7] While courts later ruled this website was an unlawful threat, all the other surveillance described was perfectly legal, even in a world where *Casey* and *Roe* remained the law of the land.[8] It's impossible to know just how many pregnant people were intimidated not to pursue abortion care through surveillance, even though it's their right.

Doctors aren't just targets of surveillance, they surveil pregnant people, too. Medical staff are effectively deputized as criminal investigators, drug testing pregnant patients without a warrant or consent, and reporting results to the police.[9] Those who test positive for controlled substances may

[4] Clapman, "Privacy Rights and Abortion Outing."
[5] Clapman, "Privacy Rights and Abortion Outing."
[6] Kate Dries, "Pro-Life Activists Are Tracking License Plates of Abortion Patients," Jezebel, August 13, 2014, https://jezebel.com/pro-life-activists-are-tracking-license-plates-of-abort-1620983363.
[7] David S. Cohen and Krysten Connon, *Strikethrough (Fatality): The origins of online stalking of abortion providers*, SLATE (May 21, 2015, 3:38 PM), https://slate.com/news-and-politics/2015/05/neal-horsley-of-nuremberg-files-died-true-threats-case-reconsidered-by-supreme-court-in-elonis.html.
[8] Planned Parenthood of Columbia/Willamette, Inc. v. Am. Coal. of Life Activists, 290 F.3d 1058, 1088 (9th Cir. 2002), as amended (July 10, 2002).
[9] Howard, "The Pregnancy Police."

face lengthy prison sentences for endangering their fetus, with their healthcare providers almost always providing the evidence against them.[10] Such healthcare surveillance would only expand further in a post-*Roe* world, drafting America's doctors and nurses to become police officers, destroying any trust between doctors, nurses, and patients.

III. Current Digital Surveillance of Pregnant People

Even with reproductive rights protected as a matter of Constitutional law, American police and prosecutors already deploy digital surveillance techniques to track and prosecute pregnant people. The trend has been accelerated both by the growing ubiquity of digital platforms in American life and reduced access to in-person abortion services. With many anti-abortion lawmakers successful in reducing the number of abortion providers in their states in recent years, and with mifepristone (also known as RU486) and other abortifacients increasingly available for terminating a pregnancy, many abortion seekers have become increasingly dependent on the internet to access abortion care.

Internet search engines are a particularly potent tool for tracking pregnant people. Police can not only obtain search histories from a pregnant person's device, but can also obtain records directly from search engines, and sometimes they don't even need a warrant.[11] Not only can police query individual search results, but they can potentially use geofence and keyword warrants (see below) to cast digital dragnets, identifying large numbers of potential abortion seekers. While such search history surveillance will grow in the post-*Roe* era, it's already a reality. In one 2018 case, Mississippi police used a woman's own search history to charge her with second degree murder following a miscarriage, relying on queries about miscarriages and how to purchase abortion-inducing pills.[12] Search results can provide an intimate window into pregnant people's thoughts, but they can easily

[10] Howard, "The Pregnancy Police."
[11] David Ingram, "Can the Government Look at Your Web Habits without a Warrant? Senators Hope to Clarify That.," NBC News, May 15, 2020, https://www.nbcnews.com/tech/security/can-government-look-your-web-habits-without-warrant-senators-hope-n1207936. *For cellphones, see Riley v. California*, 573 U.S. 373, 401 (2014).
[12] Cynthia Conti-Cook and Kate Bertash, "Digital Surveillance Presents New Threats to Reproductive Freedoms," *Washington Post*, December 15, 2021, https://www.washingtonpost.com/outlook/2021/12/15/digital-surveillance-reproductive-freedom/.

be misconstrued. Benign medical questions can be miscast and misconstrued as part of an effort to terminate a pregnancy, even when it actually ended unintentionally.

Electronic payment records and retail sales data are also potent sources of abortion surveillance. While large numbers of abortion seekers are able to purchase abortifacients online, there is likely no way to do so anonymously, especially when the most effective medications are still only administered by prescription. In 2012, Pennsylvania officials prosecuted a mother for purchasing an abortifacient online and administering it to her teenaged daughter,[13] securing a sentence of 9 to 18 months in prison.[14] While prosecutors ultimately relied on other evidence, the digital purchase records would have been quite difficult for the defense to rebut. In 2019, the FDA successfully charged a New York City woman with illegal online sales of abortifacients, following PayPal's termination of her account.[15] Law enforcement can subpoena shopping records to prove that people bought or sold abortion-inducing medications or to prove they were pregnant in the first place. When purchasers pay with a credit card, an online account, or with an in-store loyalty card, everyday purchases—medication, pregnancy tests, prenatal vitamins, menstrual products—can become circumstantial evidence.[16] Information bought and sold by the largely unregulated data-broker industry is increasingly not only targeting pregnant people with ads, but a tool for targeting them for arrest.

As with all criminal investigations, electronic communications are a particularly potent policing tool, particularly unencrypted formats like text messages and email. In 2015, Indiana prosecutors used Purvi Patel's text messages to convict her of murder for terminating her pregnancy with abortifacients ordered from Hong Kong.[17] But text messages are just one type of electronic

[13] Emily Bazelon, "A Mother in Jail for Helping Her Daughter Have an Abortion," *The New York Times*, September 22, 2014, sec. Magazine, https://www.nytimes.com/2014/09/22/magazine/a-mother-in-jail-for-helping-her-daughter-have-an-abortion.html.
[14] Bazelon, "A Mother in Jail."
[15] Chelsea Conaboy, "She Started Selling Abortion Pills Online. Then the Feds Showed Up.," *Mother Jones*, February 2019, https://www.motherjones.com/politics/2019/02/she-started-selling-abortion-pills-online-then-the-feds-showed-up/ (It is unclear to what extent PayPal data played a role in facilitating the investigation.)
[16] *See, e.g.*, Jay Greene, "Tech Giants Have to Hand over Your Data When Federal Investigators Ask. Here's Why.," Washington Post, June 15, 2021, https://www.washingtonpost.com/technology/2021/06/15/faq-data-subpoena-investigation/.
[17] Emily Bazelon, "Purvi Patel Could Be Just the Beginning," *The New York Times*, April 1, 2015, sec. Magazine, https://www.nytimes.com/2015/04/01/magazine/purvi-patel-could-be-just-the-beginning.html.

messaging subject to search. Police can use email, social media messages, communications from video game platforms, and countless other forms of electronic messaging to track and charge pregnant people. Even more secure forms of messaging, such as the encrypted messaging apps WhatsApp and Signal, can potentially be used against pregnant people if messages are retained on their devices and police gain physical access to pregnant people's electronics.

Our electronic devices not only hold a repository of our communications and purchases, but create a log of our every movement, allowing police to reconstruct a pregnant person's visit to a pharmacy, shipping facility, or abortion clinic. Police can track cellphones and cell-enabled smart devices using cell-site location information from phone providers, though a warrant is required for prolonged searches of individuals[18] or so-called "tower dumps," which identify all devices in a location.[19] Unfortunately, it's unclear if police departments agree that a warrant is needed to obtain other location data, such as GPS location information. And when police do obtain a warrant, they often use novel court orders like "geofence warrants," which require Google and other companies to produce information on all the users in a specified time and place, whether one room or virtually an entire town.[20] Data released by Google in response to an advocacy campaign by S.T.O.P. and dozens of coalition partners[21] shows that since geofence warrants were first developed in 2018, they grew to more than 10,000 a year in 2020, accounting for more than half of all American search warrants.[22]

Opponents already use the same geofencing technology to access data from other companies,[23] targeting and messaging people visiting abortion clinics.[24] They can then use advertising databases to

[18] *Carpenter v. United States*, 138 S. Ct. 2206 (2018). The U.S. Supreme Court held in *Carpenter v. United States* that law enforcement can access individuals' cell site data with a warrant based on probable cause.
[19] *Commonwealth v. Perry*, No. SJC-13144 (Mass. Apr. 1, 2022).
[20] Jennifer Valentino-DeVries, "Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works.," *The New York Times*, April 13, 2019, sec. Technology, https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html.
[21] The Surveillance Technology Oversight Project, "Google Agrees To Civil Rights Groups' Demand For Geofence Warrants Report," August 19, 2021, https://www.stopspying.org/latest-news/2021/8/19/google-agrees-to-civil-rights-groups-demand-for-geofence-warrants-report.
[22] Google, "Supplemental Information on Geofence Warrants in the United States," n.d., https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf.
[23] Coutts, "Anti-Choice Groups Smartphone Surveillance."
[24] Coutts, "Anti-Choice Groups Smartphone Surveillance."

obtain "the names and addresses of women seeking abortion care, and those who provide it."[25] The practice remains lawful in 49 states, with only Massachusetts banning geofencing near abortion clinics.[26]

III. Digital Surveillance of Pregnant People Post-*Roe*

At the time of publication, a leaked draft Supreme Court opinion from *Dobbs v. Jackson Women's Health Organization* strongly suggests that justices are poised to eliminate any federal constitutional right to abortion care.[27] The fall of *Roe* will trigger 18 new or existing abortion bans,[28] transforming the internet into the last source of medically-accurate abortion information, care, and support for millions of Americans.[29] Unfortunately, police and prosecutors will respond with all the tools of modern surveillance and American policing, surveilling pregnant peoples' bodies on a scale that was inconceivable in 1973.

Prosecutors will obtain geofence warrants to track those at reproductive health clinics, even clinics out of state. Investigators will use keyword search warrants to identify everyone searching for abortion clinics, abortifacients, and even medically accurate information about abortion care.[30] Librarians and school officials will be forced to weaponize existing internet filtration and monitoring software to identify those researching abortion, turning students and patrons into suspects for merely trying to learn.[31]

---

[25] Coutts, "Anti-Choice Groups Smartphone Surveillance."
[26] Lil Kalish, "Meet Abortion Bans' New Best Friend: Your Phone," *Mother Jones*, February 16, 2022, https://www.motherjones.com/politics/2022/02/meet-abortion-bans-new-best-friend-your-phone/.
[27] Josh Gerstein and Alexander Ward, "Supreme Court Has Voted to Overturn Abortion Rights, Draft Opinion Shows," *POLITICO*, May 2, 2022, https://www.politico.com/news/2022/05/02/supreme-court-abortion-draft-opinion-00029473.
[28] Allison McCann and Taylor Johnston, "Where Abortion Could Be Banned Without Roe v. Wade," *The New York Times*, May 3, 2022, https://www.nytimes.com/interactive/2022/us/abortion-bans-restrictons-roe-v-wade.html.
[29] Conti-Cook and Bertash, "Digital Surveillance New Threats."
[30] Jessica Grose, "These Laws Are Making Miscarriage More Traumatic in America," *The New York Times*, April 27, 2022, https://www.nytimes.com/2022/04/27/opinion/abortion-laws-miscarriage.html.
[31] Albert Fox Cahn, "The Most Devastating Tool of Abortion Bounty Hunters in Texas Could Be the Surveillance State," *Fast Company*, September 14, 2021, https://www.fastcompany.com/90675851/abortion-bounty-hunters-texas-surveillance.

The fall of *Roe* and *Casey* will also expand the threat of private abortion bounty-hunter laws, which allow private litigants to sue anyone who facilitates an abortion. Currently, Texas's statute (SB8) bars any action by state officials to enforce the measure, but soon police and private bounty hunters will work in tandem to target everyone who facilitates abortion care.[32] Multiple states have either passed[33] or introduced[34] copycat measures, and the practice is likely to only increase. This is because civil claims can be pursued with much less evidence than is needed to enforce criminal abortion bans. And police and prosecutors may use their surveillance powers to assist private bounty hunters, who already are able to weaponize sprawling commercial surveillance products and open-source intelligence platforms.[35]

IV. What States Are Doing to Repel Abortion Surveillance

Numerous state laws provide some protection for pregnant people's privacy, but much more will be needed in the post-*Roe* era. Many federal and state laws protect abortion seekers' privacy by mandating access to abortion clinics and creating buffer areas around facilities.[36] These barriers not only protect physical access, but can limit visual tracking of abortion seekers. A smaller number of states also protect minors' and young adults' access to abortion by redacting sensitive data from health insurance records. However, the Supreme Court already struck down one Massachusetts buffer law on free speech grounds, and other state protections may face similar challenges.[37]

Some of the most promising state protections for abortion seekers come from more targeted bans on electronic surveillance, which don't face the equivalent constitutional challenge. One New York State measure, if passed, would not only create the country's first ban on geofence warrants and

[32] An Act Relating to Abortion, Including Abortions after Detection of an Unborn Child 's Heartbeat; Authorizing a Private Civil Right of Action," Pub. L. No. S.B. 8
n.d.), https://capitol.texas.gov/tlodocs/87R/billtext/pdf/SB00008H.pdf
[33] Keith Ridler, "Idaho Governor Signs Abortion Ban Modeled on Texas Law," *ABC News*, March 23, 2022, https://abcnews.go.com/Health/wireStory/idaho-governor-signs-abortion-ban-modeled-texas-law-83628634.
[34] Mary Kekatos, "Oklahoma Governor Signs 6-Week Abortion Ban into Law," ABC News, May 3, 2022, https://abcnews.go.com/Health/oklahoma-governor-signs-week-abortion-ban-law/story?id=84395778.
[35] Cahn, "The Most Devastating Tool."
[36] Adam Beam, "California Governor Signs Privacy Laws for Abortion Patients," PBS NewsHour, September 22, 2021, https://www.pbs.org/newshour/politics/california-governor-signs-privacy-laws-for-abortion-patients.
[37] *McCullen v. Coakley*, 573 U.S. 464, (2014).

keyword warrants, it would also ban police from purchasing such geolocation data from commercial vendors.[38] New York State is also targeting the threat that fake police social media accounts pose to pregnant people.[39] Currently, officers can manage large numbers of fake accounts through internet attribution management systems, getting members of the public to accept officers as "friends" so police can access private information without a court order.[40] This tactic will be particularly powerful post-*Roe*, when officers are able to identify pregnant people through fake reproductive health provider accounts, tricking abortion seekers to identify themselves. New York's legislation would not only forbid police from generating a false account, it would bar officers from coercing New Yorkers to provide their social media account credentials.

While rights-protective states like New York are likely to only enhance statutory protections for abortion, their local police may still facilitate abortion prosecutions. This is because federal/state and interstate data sharing agreements allow and require local police to share intelligence with federal, state, and local partners from across the country. In a post-*Roe* world, particularly in the event an anti-choice candidate wins the presidency, these sharing agreements would facilitate surveillance both of New York residents and out-of-state abortion seekers traveling to the state. As a result, states can dramatically mitigate the surveillance threat to pregnant people in their jurisdictions by withdrawing from information-sharing agreements, intelligence fusion centers, interagency task forces, and other partnerships with federal and out-of-state law enforcement. Such withdrawal would also respond to ongoing demands to limit information sharing that targets undocumented residents.[41] Currently, police in self-proclaimed sanctuary jurisdictions provide data to out-of-state and federal partners that facilitate deportation and immigration enforcement.[42]

[38] "Location Tracking Ban," S.T.O.P. - The Surveillance Technology Oversight Project, updated February 12, 2022, https://www.stopspying.org/location-tracking.
[39] https://www.nysenate.gov/legislation/bills/2021/s9247
[40] New York City Police Department, "Internet Attribution Management Infrastructure: Impact and Use Policy," April 11, 2021, https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/internet-attribution-management-infrastructure-nypd-impact-and-use-policy_4.9.21_final.pdf.
[41] Albert Fox Cahn, "Surveillance by Sanctuary Cities Is Helping ICE Track Undocumented Immigrants," NBC News, July 9, 2019, https://www.nbcnews.com/think/opinion/surveillance-sanctuary-cities-helping-ice-track-undocumented-immigrants-ncna1027981.
[42] Cahn, "Surveillance by Sanctuary Cities."

Lastly, states can also take steps to ban private-sector data brokers from buying or selling information about reproductive health. Currently, police can easily purchase information where they are unable to obtain a court order. Such a measure could follow the example of Illinois, which broadly protects biometric data through the Biometric Information privacy Act of 2008 (BIPA).[43] While BIPA does not currently include abortion-related information, an expanded statute could easily bar private companies from collecting, using, or selling abortion data without explicit, written consent. An even more aggressive law could bar use or sale of the data even with consent, barring firms from coercing pregnant people to reveal protected information.

VI. Private-Sector Privacy Protections For Pregnant People and Abortion Providers

The coming wave of abortion surveillance may be driven by dark ages ideology, but it will inspire many pregnant people to "go dark" in the modern sense of the term, hiding their electronic records through encryption and other safeguards. While digital privacy protections will never be as strong as constitutional protections, technical safeguards can powerfully protect pregnant people and those who support them.

Abortion providers and others seeking to protect pregnant people must make privacy a priority. A recent review found that Planned Parenthood, a leading reproductive health provider, had nearly 70 ad trackers and third-party cookies on its website, revealing the identities of visitors to an array of ad brokers.[44] While this user data is already invasive, it could easily become the target of a criminal inquiry in the future, whether that data is purchased by police or seized through a court order. While abortion providers have complete discretion over whether to collect user data, once they have it, employees face incarceration if they refuse to hand data over to police when ordered. Even if such entities cease all operations in anti-abortion jurisdictions, they still risk arrest for refusing to comply with a valid out-of-state court order. However, providers can protect themselves and their patients by implementing privacy-by-design principles into their digital platforms, only collecting data that's absolutely necessary for their services, retaining it only as long as needed, and minimizing third-party

[43] Illinois Biometric Information Privacy Act (BIPA) of 2008, 740 ILCS 14.
[44] Alfred Ng and Maddy Varner, "Nonprofit Websites Are Riddled With Ad Trackers – The Markup," October 21, 2021, https://themarkup.org/blacklight/2021/10/21/nonprofit-websites-are-riddled-with-ad-trackers.

sharing. Abortion providers and other institutions should immediately conduct privacy audits of all electronic communication, including use of third-party social media and messaging services.

While many of the country's largest tech companies have been quick to voice support for pregnant employees, few have addressed how their own data is going to be used against abortion seekers. Google could largely eliminate the threat of geofence warrants, keyword warrants, and other search surveillance if it simply stopped warehousing this information. Many companies are effectively immune from geofence warrants already, either because they don't collect geolocation data, or because they don't store it in a way that can comply with a geofence warrant's demands. Such privacy protections would certainly impact Google's core business offerings, but that sacrifice makes these changes the most meaningful measure of whether the company truly supports reproductive access.

Meta (Facebook's parent company) and Apple both face significant design choices for encrypted services. Currently, both companies broadly advertise encryption protections, while actually making compromises that facilitate law enforcement surveillance.[45] In recent years, Meta prominently advertised "end-to-end" encryption as a feature in its WhatsApp messaging platform.[46] However, Meta continues to collect massive amounts of data from WhatsApp users, including details of when people communicate and with whom.[47] This data could easily be used by police to find those communicating with health care providers and other services. Even more concerning, WhatsApp includes content moderation tools that allow its staff to effectively circumvent encryption and read message content.[48] Sadly, this is not nearly as insecure as Meta's other platforms, including Facebook and Facebook Messenger, which offer no default encryption protection at all.[49] Recently, the company offered limited encryption protections on Facebook Messenger, but only if users go

[45] Albert Fox Cahn and Evan Selinger, "Apple's Privacy Mythology Doesn't Match Reality," *Wired*, August 11, 2021, https://www.wired.com/story/opinion-apples-privacy-mythology-doesnt-match-reality/.
[46] Jim Martin, "New WhatsApp Ads Promote End-to-End Encryption," Tech Advisor, June 14, 2021, https://www.techadvisor.com/news/social-networks/whatsapp-message-privately-3805518/.
[47] Lily Hay Newman, "WhatsApp Communities Add New End-to-End Encryption Chat Features," *Wired*, April 14, 2022, https://www.wired.com/story/whatsapp-communities-feature/.
[48] Whitney Kimball, "WhatsApp Moderators Can Read Your Messages," *Gizmodo*, September 7, 2021, https://gizmodo.com/whatsapp-moderators-can-read-your-messages-1847629241.
[49] Jack Wallen, "How to Enable End-to-End Encryption in Facebook Messenger," TechRepublic, February 9, 2022, https://www.techrepublic.com/article/how-to-enable-end-to-end-encryption-in-facebook-messenger/.

through a cumbersome process to opt-in.[50] Collectively, these platforms will become one of the primary ways police identify abortion seekers, that is, unless Meta implements true end-to-end encryption and data minimization practices on all platforms. Currently, it has placed plans for more thorough end-to-end encryption on hold.[51]

Similarly, Apple will need to decide whether to strengthen its encryption practices or see its devices become a policing tool for pregnant people. Apple often advertises the privacy of its products, but its cloud services remain very vulnerable to a court order.[52] Since Apple retains access to all user data on iCloud, any backups stored to the service are also potentially accessible to police.[53] Even worse, Apple encourages users to save copies of encrypted communications from its iMessage service, making them vulnerable to police as well.[54] While users are told that iMessage conversations are protected from everyone else, even Apple, these protections vanish as soon as users back up data to Apple's iCloud service.[55] Additionally, Apple location tracking—including *Find My* software and AirTags hardware—are completely vulnerable to a warrant.[56] To protect pregnant people, Apple would need to completely change its encryption methodology for cloud services, ensuring that users, and only users, have the keys to their own data.

Amazon and other retailers will have to closely examine how they store, aggregate, and share purchase data. While these companies are subject to strict record-keeping requirements for all prescription medications, they may gain greater latitude on mifepristone sales data if the FDA cedes to public pressure to make the abortifacient an over-the counter medication.[57] Additionally, online retailers are likely to see purchase data scoured for information on the sale of other medications and supplements that can be used off label (without FDA approval) to terminate a pregnancy. As anti-

[50] Wallen, "End-to-End Encryption in Facebook Messenger."
[51] "Meta Response: End-to-End Encryption Human Rights Impact Assessment," April 2023, https://about.fb.com/wp-content/uploads/2022/04/E2EE-HRIA-Meta-Response.pdf.
[52] Cahn and Selinger, "Apple's Privacy Mythology."
[53] Cahn and Selinger, "Apple's Privacy Mythology."
[54] Cahn and Selinger, "Apple's Privacy Mythology."
[55] Cahn and Selinger, "Apple's Privacy Mythology."
[56] Apple, "Legal Process Guidelines: Government & Law Enforcement within the United States," n.d., https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf.
[57] "Over-the-Counter Medication Abortion," Advancing New Standards in Reproductive Health (ANSIRH) at the University of California San Francisco, accessed May 11, 2022, https://www.ansirh.org/research/ongoing/over-counter-medication-abortion.

abortion states crackdown on information about, and internet access to, approved abortifacients, increasing numbers of abortion seekers are likely to turn to these much riskier drugs and supplements.

Health data apps, particularly period trackers, are a potent source of data for police. While period trackers are an indispensable tool for millions of Americans, they are now also a government watchdog in the making. While no app can be perfect, privacy protective apps can provide greater safety in the future. Security can be improved by storing data locally in a user's device or ensuring that only a user has access to remotely stored data. By using end-to-end encryption for cloud data, without any ability for the app provider to reset the password or bypass the encryption key, the company can limit its ability to comply with a court order. Providers can further protect users by forgoing any collection of aggregated "anonymous" user data,[58] and only retaining user data for the minimum time period needed for the app to function. As a best practice, health apps could install a so-called "warrant flag" to notify if the app is subject to government surveillance.[59]

Lastly, retailers have long been uniquely positioned to identify pregnant people through their own customer tracking tools. More than a decade ago, Target received national attention for identifying that a teenage customer was pregnant before her own father knew, simply through changes in consumer behavior.[60] Retailers find it quite lucrative to predict new pregnancies, so expectant parents can be targeted for ads at a moment their consumption is likely to dramatically expand.[61] But such commercial marketing lists now will become evidence for those individuals whose pregnancies don't come to term. Even where companies don't sell such data, police will likely target them, using

[58] Many companies collect detailed records about user behavior (when they use an app, how long, etc.) and then strip away users' name and email address, labeling the data "anonymous." But even this deidentified data can frequently be re-identified by third parties, especially if the company is ordered to do so. Even a change in the frequency with which a user accesses the app could become evidence.
[59] A "warrant flag" is an automated message warning users when the system is being monitored by the government. Such a system is indispensable when operators receive a warrant that includes a gag order, preventing them from notifying users. However, when operators already have a warrant flag system installed, an automated warning will go out whenever they fail to take action and reset a periodic timer. While the government can order operators to remain silent, they legally can't force operators to reset warrant flags, making it a lawful way to communicate.
[60] Charles Duhigg, "How Companies Learn Your Secrets," *The New York Times*, February 16, 2012, sec. Magazine, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.
[61] Duhigg, "How Companies Learn Secrets."

a methodology similar to geofence warrants. The answer for retailers is clear: don't keep the data and don't create the lists.

Privacy Practices for Pregnant People

When it comes to privacy, it's truly one size fits none. Every pregnant person and abortion seeker will face unique surveillance threats and have different resources at their disposal. While it is impossible to fully eliminate the threat that tracking poses, threat modeling allows individuals to identify the steps that they should prioritize in protecting their privacy. Individuals can begin by listing the items that create the greatest privacy risk, and prioritizing those where the simplest solutions are available, working down the list to those risks that are less acute and harder to solve.

Internet activity generally, and web-browsing specifically, will always be subject to expansive government and private tracking. Pregnant people can gain additional modest protections by employing a virtual private network (VPN), creating a layer of encryption between users and their network providers. This is particularly important when using insecure, shared networks, such as at a coffee shop, airport, or sometimes even at home (if the home network is managed by someone the user fears being monitored by).

A VPN will also mask users' internet protocol (IP) address from the website or service they're interacting with, obscuring their location as well. However, sites can use a variety of other methods to identify users, including cookies, ad trackers, and browser fingerprinting.[62] Additionally, when using a VPN, internet activity remains visible to the VPN operator, some of which commercialize user data or cooperate with law enforcement.[63]

Users can gain additional privacy protections by using The Onion Reuter (TOR) network.[64] Unlike a VPN, which routes internet activity through a single server, TOR routes content through a series of

[62] Browser fingerprinting frequently can identify your browser's unique identity based on hardware specifications, system fonts, plugins, and other factors.
[63] Electronic Frontier Foundation, "Choosing the VPN That's Right for You," Surveillance Self-Defense, March 7, 2019, https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.
[64] "The Tor Project," accessed May 11, 2022, https://torproject.org.

three intermediary servers. This approach masks user IP addresses both from the service they communicate with and the servers in between. Additionally, the intermediary servers have reduced capacity to view users' internet activity, unlike a traditional VPN. In addition to the TOR network, TOR offers a web browser that eliminates many factors used in browser fingerprinting and other forms of tracking, further improving anonymity.[65] While using a VPN, TOR, or the combination of the two can reduce third party tracking, no tool can grant users perfect anonymity, and law enforcement actively works to compromise these technologies.

Traditional SMS text messages and unencrypted social media messages can be readily intercepted. Using a messaging tool with end-to-end encryption can block third parties, even law enforcement, from accessing the content of messages. While many messaging platforms offer some level of encryption, at the time of publication, Signal provides the most robust security.[66] Still, no message is truly secure if it's retained on a device. By enabling auto-delete / disappearing messages, users can reduce the amount of data exposed if their or their correspondent's device is later compromised.

While cellphones may be a ubiquitous part of modern life, they also enable an inescapable network of tracking. Between cell site location information, GPS, Bluetooth and Wi-Fi network proximity data, and countless other datapoints, it's impossible to fully mask your location when using a cellphone. While disposable cellphones can provide greater protection from location tracking, they can easily be connected to the user unless purchased and used securely.[67] Even a single message can connect a "burner" phone to its owner's identity.

Almost all electronic payments are readily traced and identified by law enforcement. Decades of anti-money-laundering infrastructure has built up a sprawling surveillance infrastructure for nearly any form of non-cash payment. Increasingly, police can track large volumes of crypto currency

[65] "The Tor Project: Download," accessed May 11, 2022, https://torproject.org.
[66] "Signal Messenger: Speak Freely," Signal Messenger, accessed May 11, 2022, https://signal.org/en/index.html.
[67] Police are frequently able to trace ownership of pre-paid, disposable cellphones, but users can make this more difficult by purchasing phones in cash, from a store with limited or no surveillance, located far from the purchaser's frequented locations. Additionally, activating a phone at your home, office, or other associated addresses and/or using it to communicate with known contacts can also help police identify the device.

transactions, identifying parties even years after the fact.[68] For sensitive transactions, cash remains the most privacy-protective option. However, financial institutions are required to report any financial transaction exceeding $10,000,[69] and it is a federal offense to structure payments to purposefully avoid the $10,000 reporting threshold.[70]

These are just some of the steps that pregnant people can take to protect their privacy in the post-*Roe* era, but far more is needed. Sadly, no privacy self-help can provide abortion seekers with the level of protections that *Dobbs* will soon roll back.

VII. Conclusion

When *Roe* is likely overturned, we will enter a truly unprecedented period, one where reproductive health is policed with the full might of the American surveillance state. Every aspect of life will become more trying for pregnant people, even those fortunate enough to live in rights-protective states like New York. And every aspect of pregnant people's digital lives will be put under the microscope, examined for any hints that they sought (successfully or otherwise) to end their pregnancy.

With state officials poised to pursue charges under America's more than 4,400 abortion laws,[71] they will turn to the surveillance tools that have become so central to American policing, using technology to peer into the most intimate aspects of our lives. Already, reduced abortion care has deadly consequences for pregnant people in America, with many turning to dangerous folk

---

[68] Brett Wolf, "US Law Enforcers Partner with Cryptocurrency Tracking Firm to Fight Financial Crime," *Thomson Reuters*, December 23, 2020, sec. Investigation Fraud & Risk, https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/cryptocurrency-financial-crime/.

[69] Internal Revenue Service, "Cash Payment Report Helps Government Combat Money Laundering | Internal Revenue Service," February 2019, https://www.irs.gov/newsroom/cash-payment-report-helps-government-combat-money-laundering.

[70] Radley Balko, "The Federal 'Structuring' Laws Are Smurfin' Ridiculous," *Washington Post*, March 24, 2014, https://www.washingtonpost.com/news/the-watch/wp/2014/03/24/the-federal-structuring-laws-are-smurfin-ridiculous/.

[71] Martin Antonio Sabelli, et al, "Abortion in America: How Legislative Overreach is Turning Reproductive Rights into Criminal Wrongs" 3 (2021), https://www.nacdl.org/getattachment/ce0899a0-3588-42d0-b351-23b9790f3bb8/abortion-in-america-how-legislative-overreach-is-turning-reproductive-rights-into-criminal-wrongs.pdf.

remedies.[72] And others will suffer indescribably when forced to forego medical treatment for a miscarriage, fearful they will be wrongly charged with abortion and that the information they give to doctors will be used against them in a court of law.[73]

There is much that we can do to push back against this nightmare, but we must act soon. Rights-protective states must curtail the government surveillance powers that will soon be aimed at pregnant people, banning abusive tactics like geofence warrants and police data purchases. Abortion providers and advocates must harden their digital infrastructure, ensuring the privacy of pregnant people who seek their help online. Tech giants like Apple, Facebook, and Google must dramatically improve encryption and privacy protections, ending the mass police surveillance they've allowed to become commonplace.

Anti-surveillance protections will never be a complete substitute for the reproductive rights *Roe* and *Casey* safeguarded, but they are the most impactful steps that abortion supporters can take in the face of the devastating ruling expected in *Dobbs*. Pro-choice leaders will have to fundamentally challenge the role of police surveillance in the post-9/11 world, but that is the price of retaining any meaningful reproductive rights.

[72] *W. Alabama Women's Ctr. v. Miller*, 217 F. Supp. 3d 1313, 1332 (M.D. Ala. 2016).
[73] "Felony Charge Dropped Against Alabama Mother Who Renewed Valid Prescription to Manage Chronic Pain During Pregnancy," National Advocates for Pregnant Women, February 23, 2022, https://www.nationaladvocatesforpregnantwomen.org/felony-charge-dropped-against-alabama-mother-who-renewed-valid-prescription-to-manage-chronic-pain-during-pregnancy/.

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT