**POST-ROE SURVEILLANCE 12/12/22**

**A SENIOR FOCUS PROJECT BY EMMA DERMANSKY**



PHOTOGRAPH BY CHIP SOMODEVILLA/GETTY IMAGES

**HOW DOES MASS SURVEILLANCE AFFECT THE STATE OF REPRODUCTIVE RIGHTS AFTER THE FALL OF ROE V. WADE AND WHAT CAN BE DONE TO PROTECT THEM IN THE FUTURE?**

From the moment you wake up you’re being tracked. A quick check on Google Maps for train times and someone knows where you are. Privacy, the right to be left alone, is recognized by the UN as a fundamental human right. These days, unless you’re willing and able to disappear into the woods, privacy is an illusion. For hundreds of years, surveillance was the tool of governments. The technological capacity for surveillance has only grown, outpacing our 235 year old constitution. Our founding fathers could have predicted Edward Snowden’s 2013 leaks revealing NSA spying of American citizens’ emails and texts foreshadowed mass surveillance on a level Americans had never seen.

As the United States moved into the new millennium, federal agencies lost their monopoly on surveillance. With the rise of the internet and social media, surveillance became the key to making a massive profit. To keep users scrolling, companies had to figure out who their users were, in order to show them content that they liked. Everything that makes people who they are, every thought and every emotion is being harvested for data. The more users scroll, the more advertisements they see, leading to more profit for Big Tech.[[1]](#footnote-0)

The bigger the data pool, the larger the profit, but not all data is created equal. Some types of data are more lucrative than others. Specifically, data on pregnant people. A child is a major life change, and parents will need to purchase diapers, cribs and toys. Since those aren’t items they purchase regularly, they are open to changing where they purchase products from.[[2]](#footnote-1) Target is one company that took advantage of this phenomenon to reap a larger profit. Staticians designed an algorithm that would identify a user’s shopping habits and calculate the probability of pregnancy, and then save that information under a unique Guest ID.[[3]](#footnote-2) If a customer purchased brightly colored furniture, vitamin supplements, and a bag big enough for diapers, Target would calculate a high probability of pregnancy and send her advertisements for baby products. This model was so successful that Target made the news when the advertisements they sent predicted a girl’s pregnancy before her father.[[4]](#footnote-3)

After hearing about Target’s algorithm, Janet Vertesi, a sociology professor at Princeton University attempted to hide her pregnancy away from the internet. Her strategy included using cash, gift cards, and not mentioning her pregnancy anywhere online to maintain her anonymity, while relying on her family to do the same. While Vertesi’s experiment proved successful, as she made it through pregnancy without receiving any targeted ads, it proved unsustainable. Beyond the immense inconvenience, the experiment proved to be legally dubious. Gift cards purchased over a certain amount are reported to the police, making it impossible to hide a pregnancy completely.[[5]](#footnote-4)

One industry for apps and technology, coined *femtech*, is also in the business for predicting pregnancy. Femtech broadly covers technology focused on women’s health, with a large number of apps dedicated to fertility and menstrual tracking. The femtech industry grew from 57 million dollars in 2012, to 2.3 billion dollars in 2020.[[6]](#footnote-5) Millions rely on these apps, but research has led experts to believe the data these apps collect aren’t solely for their users’ benefit. A 2022 study published in JMIR[[7]](#footnote-6) researched the privacy policy of the 23 most popular femtech apps. Of those 23 apps, 14 allowed location tracking, 16 displayed a privacy policy, 3 collected data without consent, and only 13 apps gave users information on the security of their data. 20 apps shared user data with third parties[[8]](#footnote-7). Not only is in-app data vulnerable, but it's also being sent to unknown secondary locations. Once the data leaves the app, it falls out of the user’s hands and into the hands of different agents, including the government.

Femtech’s poor privacy policies are one of many reasons why activists are concerned about surveillance in the wake of the Supreme Court’s Dobbs v. Jackson decision. In their *Pregnancy Panopticon* report,Cahn and Manis write, “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.”[[9]](#footnote-8) America is entering a stage of policing never seen before, making reproductive healthcare more difficult than it has been in years. Still, despite the massive capacity for surveillance, there are some limits in place.

HIPAA, the Health Insurance Portability and Accountability Act, provides some patient privacy. It classifies certain kinds of information as protected health information (PHI). Information is only considered PHI if it is given to a HIPAA-protected entity, such as a patient’s doctor or insurance company. PHI includes treatment plans, health history, and information that could be used to identify a patient.[[10]](#footnote-9) It does not protect search history, data given to menstrual tracking apps, or geolocation data because Big Tech is not a HIPAA-protected entity.[[11]](#footnote-10) A woman telling her doctor she’s pregnant is protected by HIPAA, but the Google search into her options isn’t. The local Planned Parenthood is legally required to protect her privacy when she goes to get an abortion, but the phone in her pocket tracking her location faces no regulations.

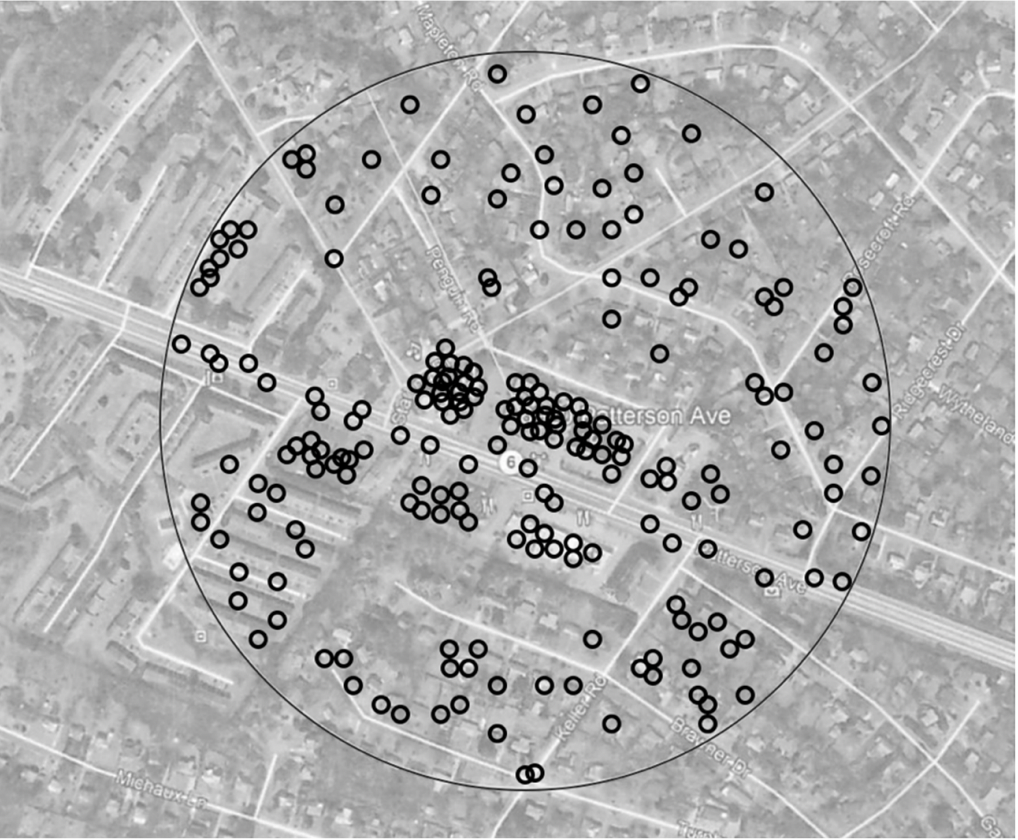
Consumer data protections on the local level can cover some of HIPAA’s blind spots. California, Colorado, Connecticut, Utah and Virginia all have consumer data protection laws in place.[[12]](#footnote-11) They give consumers the right to access the data corporations collect and opt-out of their information being sold, along with added regulations on privacy policies to provide more transparency. In the interest of protection reproductive rights, Massachusts banned the practice of geofencing around abortion clinics.[[13]](#footnote-12)

While state level protections only apply to one section of the country, federal protections cover the entirety of it. In 2018, the Supreme Court ruled when law enforcement using geolocation data to track a suspect for several without a probable cause warrant (one obtained from a judge) they violated the fourth amendment. Carpenter v. The United States is a landmark case because it rejects third-party doctrine: even though Timothy Carpenter consented to giving his location data to his cell-phone provider, his fourth amendment rights were still violated. In a world where Google’s software is practically required for modern day life, Carpenter could provide major consumer protection in a post-Roe world. However, Carpenter comes with a caveat: the court said that its decision was a narrow one, implying that the ruling doesn’t apply to all technology.[[14]](#footnote-13)

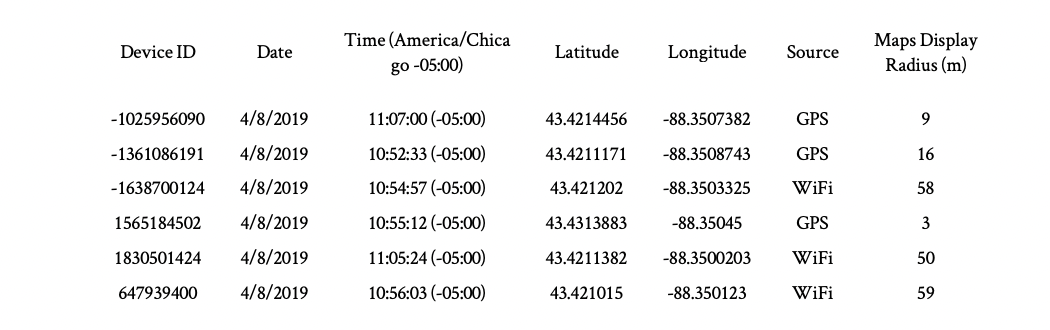
The Carpenter ruling is a new one, and courts are still figuring out how to address it. As Amster and Diel write in the Stanford Law Review, “One prominent unanswered question in this inquiry is whether the government can avoid Carpenter's warrant requirement by using many small intrusions over a large population (as it does with geofence warrants) rather than a few large intrusions over a small population (as it did in Carpenter).”[[15]](#footnote-14) Geofences are one of many types of surveillance that Carpenter does not address, leaving courts scrambling to figure out what types of surveillance are constitutional. In addition, Carpenter may not be around long enough to support lasting change. The decision came down to a 5-4 vote, and a new conservative majority puts its longevity into question.

Clearly, there is some substantial consumer and patient protection in place. We don’t live in a complete state of unregulated surveillance - just a near total one. With HIPAA’s lack of protection for search history and personal messages, the two types of digital evidence most used in prosecuting abortion seekers, along with Carpenter’s limits, the surveillance of pregnant people remains largely unimpeded.

85% of all Americans carry smartphones with them, and all of those smartphones are capable of location tracking.[[16]](#footnote-15) With billions of data points, sorting raw geolocation data would take up all of law enforcement’s time. Enter geofences, a type of digital parameter that collects all location data in a certain area at a certain time. Geofences can span long distances and time - a requested geofence in 2019 covered 7.4 acres for nine hours.[[17]](#footnote-16) Geofences were originally designed for precise advertising. Google’s geolocation database, the SensorVault, is used for targeting advertisements and determining store traffic. It's also an enormously helpful tool for law enforcement.



A visual model of a geofence surrounding a Dollar Tree[[18]](#footnote-17)



Geofence data from a bank robbery investigation in Wisconsin.[[19]](#footnote-18)

Police get geofence data through geofence warrants. Geofence warrants are growing at an exponential rate: In 2018 Google received 982 geofence warrants, an increase of 1,500% since 2017, and in 2020 they received 11,554 warrants. Texas, a state with a complete abortion ban, requested 1,825 of the 20,932 requests Google received within three years.[[20]](#footnote-19)

Obtaining a Geofence doesn’t require any judicial oversight, and neither does deanonymizing the data. Location data can reveal incredibly personal information, and finding the name behind the smartphone is not difficult. Law enforcement can get unmask devices through Google[[21]](#footnote-20) or other advertising databases[[22]](#footnote-21). Google has their own jurisdiction when it comes to complying with Geofence warrants, but with the fall of Roe law enforcement in anti-abortion states will become more emboldened. With abortion totally or near totally banned, it will be easy to argue probable cause when requesting geofence warrants for reproductive health clinics, both in and out of state.[[23]](#footnote-22)

Even if everyone left their phones at home, geolocation tracking would not stop. Automated License Plate Trackers (ALPRs) can be found all across the country. Cameras on street poles and highway overpasses are always recording license plate data. They’re commonly used to identify stolen cars and issue tickets, but they could just as easily be utilized to track people seeking reproductive care. It’s one more way of knowing where people are, and ALPR companies have close relationships with law enforcement across the country.[[24]](#footnote-23) The Company Flock claims it has cameras in 1500 cities and captures data from over one billion vehicles per month. Jay Stanley, ACLU Senior Policy analyst said, “It’s a giant, nationwide mass surveillance system. That obviously has serious implications should interstate travel become part of forced-birth enforcement.”[[25]](#footnote-24) One reason today’s mass surveillance is so effective is because there is not just one surveillance system in play - there are several.

As the surveillance of search history grows, so does the amount of people seeking health information online: “Like everyone else seeking information online, they [pregnant people] prefer the online experience because of the decreased costs, the appeal of not traveling, and having the ability to manage their health in what feels like a private manner. While the online environment gives the seeker of medical information a feeling of privacy, internet use is actually easily surveilled. Every mouse or finger hover, click, keystroke, pause, and purchase is recorded and tracked.”[[26]](#footnote-25) People rely on the internet for healthcare, and they are completely unprotected. Access to an individual’s search history can reveal deeply personal information, and police have easy access to it.[[27]](#footnote-26)

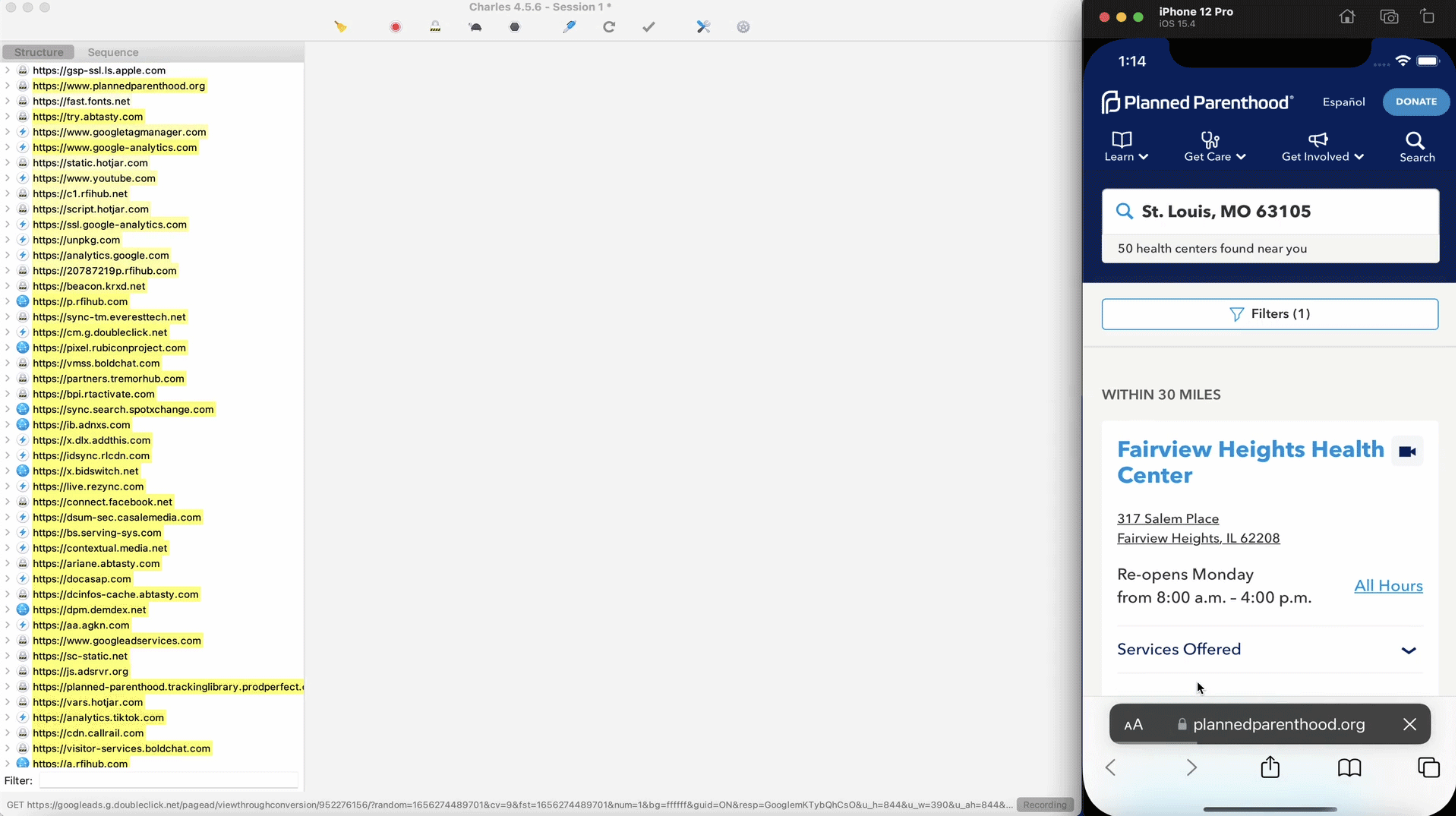
Individuals' search history can be subpoenaed along with mass groups of people’s search history through keyword warrants. Police could issue a keyword warrant on “abortion” casting a digital dragnet across the internet that would identify abortion seekers. Just like Geofences, Keyword warrants find evidence that lead to suspects, rather than the other way around.

In tens of thousands of schools, software like GoGuardian and Bark are monitoring everything students do on their computers. Whenever the software’s algorithm flags dangerous behavior, like a suicide threats, alerts are sent out to adminstraitors, parents, and police.[[28]](#footnote-27) Add abortion related keywords to the software flagging althrogithm’s and police wouldn’t need to use keyword or geofence warrants to track down abortion seekers because schools would be doing the work for them.

GoGuardian reports alerts for “sexual content” on student computers straight to the police. Flagging algorithms are not entirely accurate. Securly, another student surveillance company, was flagging sexual health resources as pornography.[[29]](#footnote-28) With the massive level of surveillance, advocates worry students won’t be able to access health information they need, such as the fact that Plan B has a weight limit.[[30]](#footnote-29) Teenagers should be able to access sexual education resources, including information on abortion, without being reported to the police.

Without end-to-end encryption, digital messages can easily be surveilled by law enforcement. Facebook Messenger only recently started rolling out opt-in encryption. Even the companies that advertise end-to-end encryption have back doors for law enforcement surveillance. Whatsapp, advertised to have end to end encryption, still collects data on who users are communicating with, and has moderation tools that let staff read the content of flagged messages. While iMessages on Apple phones are encrypted, backups of conversations on iCloud are not.[[31]](#footnote-30) Apps like Signal, which are fully end-to-end encrypted, are not used at the scale of iMessage or Facebook Messenger.

It’s not just tech companies claiming to care about privacy that have a back door for surveillance. Nonprofits on the front lines of the fight for reproductive rights have trackers littered across their websites. In June, the Washington Post reported that Planned Parenthood’s scheduling tool shared data with Big Tech companies.[[32]](#footnote-31) Lockdown Privacy’s investigation discovered that information was being shared with Google, Facebook, Tiktok, and Hotjar.[[33]](#footnote-32) Data shared included IP addresses, zip codes and the type of care users requested.



Trackers found on Planned Parenthood’s Scheduling tool by Privacy Lockdown[[34]](#footnote-33)

Hey Jane, a company that provides accessible abortion pills also had trackers on their website. Using their Blacklight Privacy Inspector, the Markup found trackers that notify Google and Facebook about the web activity of visitors, along with user reviews containing personal information.[[35]](#footnote-34)

After being contacted by The Markup, Hey Jane removed some of its analytics trackers, including one designed by Meta. They also deleted user reviews from their website. Five days after the Washington Post, Planned Parenthood argued no PHI had been breached, but agreed to remove marketing pixels on their search page.[[36]](#footnote-35)

The possibilities for surveillance have become so huge that they can begin to feel hypothetical, but they have a very real impact on the women that have been put on trial. Both before and after the fall of Roe, digital evidence has been used to charge women seeking illegal abortions.

In 2015 Purvi Patel’s text messages gave Indiana prosecutors the evidence they needed convict her for murder after she terminated her pregnancy with abortion pills from Hong-Kong[[37]](#footnote-36). Patel was initially sentenced to twenty years in prison, with an appeal shorting it to three.[[38]](#footnote-37) Without Patel’s private communications, it would have been much harder for such a large sentence to be given.

Latice Fisher faced similar persecution in 2017, when after being rushed to the hospital for a miscarriage, she was investigated for infanticide. Mississippi's case against Fisher rested on her search history. Prosecutors argued that because Fisher searched for “How to induce a miscarriage,” and purchased abortion pills online, she committed second-degree murder, even though she would have been unable to terminate her prenancy during the third trimester.[[39]](#footnote-38) Fisher faced 20 to 40 years in prison and the possibility of a life sentence was tangible. With support from grassroots activists, all of the state's changes were dismissed, but Fisher’s case serves as a stark reminder of the power of digital evidence. The only proof Missipi had to convict Fisher for murder was her search history, which wasn’t enough to prove she had abortion in the first place. As Conti Cook writes, “Miscarriages naturally terminate up to 21% of pregnancies after week five and as many as 75% of pregnancies before week five; thus, it is not uncommon for a woman contemplating an abortion to coincidentally suffer a miscarriage.”[[40]](#footnote-39)

Both of these women were charged when the federal protections from Roe v. Wade still existed. Post-Roe, less legal protection exists while digital surveillance grows. A month after the overturning of Roe v. Wade, Seventeen-year-old Celeste Burgess was arrested and charged with undergoing an abortion over 20 weeks after conception, a crime in Nebraska. Just like in Fisher’s case, Burgess was prosecuted using digital evidence.

Burgess originally claimed she experienced a miscarriage, but when Nebraskan law enforcement received a tip, they got a warrant to access her Facebook account and discovered a chat conversation with her mother detailing how Burgess planned to have a self-managed abortion. Within nine days, the police had permission to raid her home.[[41]](#footnote-40) Burgess is currently awaiting trial, with nearly no legal protection for her right to privacy or reproductive choice.

In all these cases, digital evidence collected through mass surveillance was used by anti-choice law enforcers sentance abortion seekers to longer jailtime. As Conti-Cook writes, “Digital evidence fills a gap for prosecutors keen on prosecuting women for their pregnancy outcomes. When medical theories fail to explain why some outcomes happened, prosecutors can now sift through an accused person’s most personal thoughts, feelings, movements, and medically-related purchases during their pregnancy, even if there is little evidence supporting the conclusion that their conduct caused the pregnancy to end.”[[42]](#footnote-41) Before they had access to digital evidence, testimony from Doctors and Nurses was all prosecutors had access to. Now, the personal nature digital evidence allows prosecutors to argue an intent to kill, something required for more severe murder charges with high jail time.

With digital evidence as an invaluable tool for anti-abortion agents, the collectors of that data have been under increasing scrutiny. Big Tech has been forced on the defensive for their data collection, something integral to their business.

When Meta was criticized for handing over texts to Nebraska police, they published a post in the Meta Newsroom stating “Much of the reporting about Meta’s role in a criminal case against a mother and daughter in Nebraska is plain wrong.”[[43]](#footnote-42) Meta says they received “valid legal warrants on June 7th”, weeks before the Supreme Court decision. It was requested that Meta hand over the data, and abortion was not mentioned anywhere in the warrants they were given. Everything they did was legal, and they may have gotten in legal trouble should they have rejected Nebraska’s warrant.

Ten years ago, when statistician Andrew Pole was questioned about the ethics of Target’s tracking of pregnant women, he said, “We are very conservative about compliance with all privacy laws. But even if you’re following the law, you can do things where people get queasy.”[[44]](#footnote-43)

Big Tech’s views on privacy today are largely similar. Companies are making sure consumers know they are following the law. In July, Google published a blog post titled: “Protecting People’s Privacy on Health Topics,”[[45]](#footnote-44) where it reminds users of how they handle law enforcement requests for user information, “We take into account the privacy and security expectations of people using our products, and we notify people when we comply with government demands, unless we’re prohibited from doing so or lives are at stake — such as in an emergency situation. In fact, we were the first major company to regularly share the number and types of government demands we receive in a Transparency Report.”[[46]](#footnote-45) Google is prioritizing reassuring users that their data is in safe, transparent hands at a time when data is a very dangerous commodity.

Along with legal transparency, tech companies have moved to empower the reproductive rights of individuals, showing support for the cause. In the immediate aftermath of the Dobbs decision, companies including Microsoft, Meta Google, EBay, Zillow, Netflix, Mozilla, Airbnb, and Snapchat , announced that they would cover travel and medical fees of employees seeking reproductive care.[[47]](#footnote-46) Google announced users would have the option to mass delete menstrual data collected on Fitbits, and Meta announced plans to make encryption the default for their messaging apps in 2023.[[48]](#footnote-47)

Even if Big Tech took no action to protect abortion seekers’ data, the arguement remains that when users consent to giving up their data, Big Tech can do whatever they want with it. This is known as third-party doctrine: When users give away information to third parties, they lose control of it. Accepting Google’s privacy policy is a choice, and by clicking agree, users forfeit their rights to it. That was the basis of the Carpenter v. United States dissent, supported by four out of nine justices.[[49]](#footnote-48)

Logically, third-party doctrine makes sense. Once you look at the current reality, it becomes less reasonable. It is near impossible to avoid BIg Tech in modern day life. You may not want to agree to Google’s privacy, but you will if your job uses the Google suite. The average person does not have the time to read through 10,000 word legal documents. The average person does not stop Google from collecting location data, something Google’s engineers struggle with. [[50]](#footnote-49)

Surveillance has become something society has accepted. From our locations to our private conversations to the information we look for, everything is being recorded, either to make a profit off of us or to prosecute us. In 1973, The Supreme Court ruled that the 14th amendment’s right to privacy encompassed an indvidual’s right to decide whether or not to terminate their pregnancy. In 2022, the court ruled that reproductive health was not included in the right to privacy. In 2022, there is hardly any right to privacy at all. Even when abortion was constitutionally protected, digital surveillance of pregnant people was being used to prosecute them for seeking abortions. The Court ruled that a right to privacy protects abortion access. The reverse is also true: no right to privacy means no protection for abortion access. No matter what the federal law on abortion is, surveillance infrastructure maintains a database that can be used to prosecute pregnant people at anytime. It is impossible for people to manage their reproductive health when it is constantly being surveilled and targeted.

The state of America's privacy and reproductive rights are looking increasingly dire, making it easy to fall into cynicism. Activists refuse to take the bait. Civil rights attorney Conti-Cook looks at the example set by the Stop LAPD Spying Coalition. Organizing to protect historically marginalized communities from police surveillance, they designed the “power not paranoia,” framework for tackling the issue of surveillance. Organizations like the Our Data OUr Bodies project and the Movement Alliance Project have with them to stop further surveillance and protect their communities.[[51]](#footnote-50) Reproductive justice advocates are following their lead. New York City’s Surveillance Technology Oversight Project (S.T.O.P) published a report on reproductive surveillance including privacy practices for pregnant people, advising the use of VPNs and the TOR network, along with cash payments and encrypted messaging. The Electronic Frontier Foundation, one the biggest privacy advocacy groups in the country, is also fighting against the rise of reproductive surveillance, by empowering providers of abortion support and those seeking abortions with way to protect themselves digitally.[[52]](#footnote-51) While none of this can change the larger reality, by informing people as to what is going on and how they can fight back against it, the surveillance machine is just that much weaker. As Daly Barrnet of the EFF writes, “We are not yet sure how companies may respond to law enforcement requests for any abortion related data, and you may not have much control over their choices. But you can do a lot to control who you are giving your information to, what kind of data they get, and how it might be connected to the rest of your digital life”[[53]](#footnote-52)

Activists on the outside of Big Tech aren’t sure how data will be handled, but activists inside of it are fighting for less surveillance in a Post-Roe world. The Alphabet Union (AWU), formed by Google employees, expects Google to do more to protect reproductive rights. In a petition sent to Google executives, AWU members demand that Google take further steps to protect user privacy and fight reproductive misinformation. The AWU wants search history related to reproductive and gender-affirming care automatically erased, remove fake abortion providers from search results, and more transparency in advertising.[[54]](#footnote-53) While the corporate response has been to tell consumers that their data is being handled responsibly, activists argue that it is not responsible to collect it in the first place.

Lawyers are in the front lines of this fight in STOP, EFF, and beyond are fighting for stronger privacy protections. ACLU’s speech technology privacy and technology and privacy technology project has been focusing on post-Carpenter decisions, pushing courts to take a broader interpretation of the decision, giving vulnerable Americans greater protections. The National Association of Criminal Defense Lawyers is training defense attorneys about the role of data surveillance in the criminal justice system [[55]](#footnote-54), something that could prove invaluable when pregnant people and their allies are taken to court when seeking abortions. The issue of police surveillance is not a technological issue, but rather a legal one, and lawyers are rising to meet that challenge.

At a local level, so is policy. New York City passed the Public Oversight of Technology Act, forcing the NYPD to be transparent about its surveillance technology now and in the future.[[56]](#footnote-55) Another Bill S.T.O.P is campaigning for is one that would ban the practice of geofencing in New York.[[57]](#footnote-56) California’s 2018 Consumer Privacy Act gives consumers much more control over their personal data. New Hampshire, Virginia, Illinois, Washington, and New York, have introduced similar bills to protect consumer privacy protections when third party doctrine does not.[[58]](#footnote-57) Nevertheless, the majority of the laws being proposed and passed are in pro-choice states, rather in the anti-abortion states where people need their protection the most. Anti-abortion states don’t seem particularly inclined to passing these laws, which is why democrats in Congress have begun to investigate.

In late July, six democratic representatives launched an inquiry into Amazon, Oracle, Mobilewalla, and Near Intelligence’s handling of consumer location data.[[59]](#footnote-58) Rep. Lori Trahan of Massachusetts wrote, “When consumers use apps on their phone and quickly tap ‘yes’ on ‘use geolocation data’ pop-ups, they should not be worried about the endless sale of their data to advertisers, individuals or law enforcement. And it most certainly should not be used to hunt down, prosecute and jail an individual seeking reproductive care. Companies can take action today to protect individual rights.”[[60]](#footnote-59) Politicians on Capitol Hill are expecting Big Tech to take responsibility for anti-abortion surveillance; Democratic Senators Elizabeth Warren and Edward Markey sent letters to four companies that monitor students online urging them to consider them to stop collecting and reporting the data of students searching online for reproductive care[[61]](#footnote-60).

Beyond investing in Big Tech, there has been some major privacy legislation proposed on Capitol Hill. The Online Privacy Act would create an entire department to protect privacy rights. The Algorithmic Accountability Act would allow the Federal Trade Commission to investigate data protections in public sector algorithms. Other laws target facial recognition. The major weakness most of these laws all share is an exemption for law enforcement, making them more useful in protection consumer from corporations, not the government, something that won’t do very much for people under surveillance in anti-abortion states. The anti-abortion surveillance state can’t be fixed with anti-surveillance legeslation alone, it must also be accompanied by a push for the legalization of abortion nationwide - again. Even then, the issue of police surveillance seems to be a question the federal government wants to steer clear of, offering little protection for other groups facing police surveillance.

If you walked up to someone on the street and asked them how they felt about mass surveillance, there’s a good chance they’d say something along the lines of “Well, I have nothing to hide”. Here’s the thing: laws change. One morning Americans have a constitutional right to an abortion, the next they don’t. A couple months a go, a Google search search into abortion pills was nothing to hide. Now, it could lead to a sentence of years in prison. Until privacy is truly protected, civil rights will always come with a caveat. Fighting back against surveillance leads to a freer future for everyone, including those affected by the fall of Roe v. Wade.

1. Christopher Wylie, *Mindf\*ck: Cambridge Analytica and the Plot to Break America.* (New York: Random House, 2019), 120. [↑](#footnote-ref-0)
2. Charles Duhigg, "How Companies Learn Your Secrets." *New York Times Magazine*, February 16, 2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. [↑](#footnote-ref-1)
3. Duhigg. [↑](#footnote-ref-2)
4. Duhigg. [↑](#footnote-ref-3)
5. Cynthia Conti-Cook, "SURVEILLING THE DIGITAL ABORTION DIARY," *University of Balitmore Law Review*, Volume 50 (2020), 24. [↑](#footnote-ref-4)
6. Najd Alfawzan et al., "Privacy, Data Sharing, and Data Security Policies of Women's MHealth Apps: Scoping Review and Content Analysis," *JMIR MHealth and UHealth* 10, no. 5 (2022): https://doi.org/10.2196/33735. [↑](#footnote-ref-5)
7. Najd Alfawzan et al. [↑](#footnote-ref-6)
8. Najd Alfawzan et al. [↑](#footnote-ref-7)
9. Albert Fox Cahn and Eleni Manis, "Pregnancy Panopticon: Abortion Surveillance after Roe," *S.T.O.P*, May 24, 2022, https://www.stopspying.org/pregnancy-panopticon. [↑](#footnote-ref-8)
10. Steve Alder, “What Is Considered Protected Health Information under HIPAA?,” *HIPAA Journal*, January 2, 2022, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/. [↑](#footnote-ref-9)
11. Alder. [↑](#footnote-ref-10)
12. NSCL, “State Laws Related to Digital Privacy.” *NSCL*, June 6, 2022. https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx. [↑](#footnote-ref-11)
13. Cahn and Manis. [↑](#footnote-ref-12)
14. Haley Amster and Brett Diehl, "Against Geofences," *Stanford Law Review* 74, no. 2 (2022): 406, https://ezproxy.d-e.org:2443/login?url=https://www.proquest.com/scholarly-journals/against-geofences/docview/2646758135/se-2?accountid=35837. [↑](#footnote-ref-13)
15. Amster and Diehl, 407. [↑](#footnote-ref-14)
16. Pew Research Center, “Mobile Fact Sheet,” *Pew Research Center*, April 7, 2021, <https://www.pewresearch.org/internet/fact-sheet/mobile/>. [↑](#footnote-ref-15)
17. Amster and Diehl, 389. [↑](#footnote-ref-16)
18. Amster and Diehl, 399. [↑](#footnote-ref-17)
19. Amster and Diehl, 401. [↑](#footnote-ref-18)
20. Amster and Diehl, 390. [↑](#footnote-ref-19)
21. Amster and Diehl, 406. [↑](#footnote-ref-20)
22. Cahn and Manis. [↑](#footnote-ref-21)
23. Cahn and Manis. [↑](#footnote-ref-22)
24. Thor Benson, "The Danger of License Plate Readers in Post-Roe America," *WIRED*, July 7, 2022, <https://www.wired.com/story/license-plate-reader-alpr-surveillance-abortion/>. [↑](#footnote-ref-23)
25. Benson. [↑](#footnote-ref-24)
26. Conti-Cook, 24. [↑](#footnote-ref-25)
27. Conti-Cook, 24. [↑](#footnote-ref-26)
28. Todd Feathers, "After Dobbs, Advocates Fear School Surveillance Tools Could Put Teens at Risk," *The Markup*, July 8, 2022, https://themarkup.org/privacy/2022/07/08/after-dobbs-advocates-fear-school-surveillance-tools-could-put-teens-at-risk. [↑](#footnote-ref-27)
29. Feathers. [↑](#footnote-ref-28)
30. Feathers. [↑](#footnote-ref-29)
31. Cahn and Manis. [↑](#footnote-ref-30)
32. Tatum Hunter, "You scheduled an abortion. Planned Parenthood's website could tell Facebook.," *The Washington Post*, June 29, 2022, https://www.washingtonpost.com/technology/2022/06/29/planned-parenthood-privacy/. [↑](#footnote-ref-31)
33. Hunter, “You Scheduled an Abortion”. [↑](#footnote-ref-32)
34. Hunter, “You Scheduled an Abortion”. [↑](#footnote-ref-33)
35. Jon Keegan and Donna Tarr, "Online Abortion Pill Provider Hey Jane Used Tracking Tools That Sent Visitor Data to Meta, Google, and Others," *The Markup*, July 1, 2022, https://themarkup.org/pixel-hunt/2022/07/01/online-abortion-pill-provider-hey-jane-used-tracking-tools-that-sent-visitor-data-to-meta-google-and-others. [↑](#footnote-ref-34)
36. Tatum Hunter, “Planned Parenthood Suspends Marketing Trackers on Abortion Search Pages,” *The Washington Post,* June 30, 2022), https://www.washingtonpost.com/technology/2022/06/30/planned-parenthood-privacy-data/. [↑](#footnote-ref-35)
37. Cahn and Manis. [↑](#footnote-ref-36)
38. Conti-Cook, 50. [↑](#footnote-ref-37)
39. Conti-Cook, 49. [↑](#footnote-ref-38)
40. Conti-Cook, 51. [↑](#footnote-ref-39)
41. Emily Baker-White and Sarah Emerson, "Facebook Gave Nebraska Cops A Teen's DMs. They Used Them To Prosecute Her For Having An Abortion.," *Forbes*, August 8, 2022, https://www.forbes.com/sites/emilybaker-white/2022/08/08/facebook-abortion-teen-dms/?sh=2501927a579c. [↑](#footnote-ref-40)
42. Conti-Cook, 51. [↑](#footnote-ref-41)
43. Meta, “Correcting the Record on Meta’s Involvement in Nebraska Case”, *Meta*, August 9, 2022, https://about.fb.com/news/2022/08/meta-response-nebraska-abortion-case/. [↑](#footnote-ref-42)
44. Duhigg. [↑](#footnote-ref-43)
45. Jen Fitzpatrick, “Protecting people’s privacy on health topics.” *The Keyword,* July 1, 2022, https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/. [↑](#footnote-ref-44)
46. Fitzpatrick. [↑](#footnote-ref-45)
47. Kyle Wiggers, “Tech companies respond to US Supreme Court abortion decision” *TechCrunch*, June 24, 2022, accessed November 16, 2022, https://techcrunch.com/2022/06/24/tech-companies-respond-to-u-s-supreme-court-abortion-decision/ [↑](#footnote-ref-46)
48. Sara Su, “Testing End-to-End Encrypted Backups and More on Messenger,” *Meta,* August 11, 2022, https://about.fb.com/news/2022/08/testing-end-to-end-encrypted-backups-and-more-on-messenger/ [↑](#footnote-ref-47)
49. Sabrina McCubbin, "Summary: The Supreme Court Rules in Carpenter v. United States," Lawfare, last modified June 22, 2018, accessed December 5, 2022, https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states. [↑](#footnote-ref-48)
50. Amster and Diehl, 397. [↑](#footnote-ref-49)
51. Conti-Cook, 66-68. [↑](#footnote-ref-50)
52. https://www.eff.org/deeplinks/2022/06/security-and-privacy-tips-people-seeking-abortion [↑](#footnote-ref-51)
53. eff [↑](#footnote-ref-52)
54. Taylor Hatmaker, “Google workers call on the company to expand abortion and privacy protections.” TechCrunch, August 18, 2022, accessed November 16, 2022,

    <https://techcrunch.com/2022/08/18/google-abortion-awu-petition/> [↑](#footnote-ref-53)
55. Conti-Cook, 70. [↑](#footnote-ref-54)
56. Michael Sisitzky and Ben Schaefer, “THE NYPD PUBLISHED ITS ARSENAL OF SURVEILLANCE TECH. HERE’S WHAT WE LEARNED” *NYCLU,* February 21st, 2021, https://www.nyclu.org/en/news/nypd-published-its-arsenal-surveillance-tech-heres-what-we-learned. [↑](#footnote-ref-55)
57. Cahn and Manis. [↑](#footnote-ref-56)
58. Conti-Cook, 71 [↑](#footnote-ref-57)
59. Marcy Gordon, “Democrats widen scrutiny of tech over abortion data privacy.” *AP News*, July 22, 2022, https://apnews.com/article/abortion-technology-apple-inc-congress-government-and-politics-fa6dfd46baeb3732df4b4fcb720dd04a [↑](#footnote-ref-58)
60. Gordon. [↑](#footnote-ref-59)
61. Gordon. [↑](#footnote-ref-60)