**FOCUS PORTFOLIO**

**MASS SURVEILLANCE AFTER ROE**

**BY EMMA DERMANSKY**

TABLE OF CONTENTS

[STATEMENT OF COURSES PARTIALLY DROPPED 4](#_9srfqbn4xmsa)

[FIRST SEMESTER QUESTIONS 4](#_fuv6c7suh95y)

[FIRST-SEMESTER PAPER SYNOPSIS 4](#_vyrsbyjg0y1g)

[FIELDWORK QUESTIONS 5](#_7vp9wtuw2krx)

[FIELDWORK SITES 6](#_4mztdutg7vv1)

[HOURS PER WEEK 7](#_o697w819dp1s)

[FIRST SEMESTER BIBLIOGRAPHY 8](#_5lomh6benyx5)

[SECOND SEMESTER BIBLIOGRAPHY 11](#_vztmmx2kfzpb)

[EVIDENCE 12](#_6f1qwmq9zte7)

[NOTES 12](#_w471bpfncpfw)

[NOTES RATIONALE 12](#_1u9zi3w2k0b)

[NOTES FROM TALKING TO ABBY ABRAMS 12](#_611r6rnjh0o)

[NOTES FROM BARNARD ABORTION AS ABORTION PANEL 16](#_8utl9k25xljf)

[NOTES FROM NYCFAR ORIENTATION 19](#_px44v598m44b)

[TRANSCRIPTS 22](#_nhf8e3y0lepb)

[TRANSCRIPTS RATIONALE 22](#_wzeyieuk5b1t)

[SNIPPET FROM A CONVERSATION WITH ABBY ABRAMS 22](#_j95q661cktqi)

[SNIPPETS FROM AN INTERVIEW I DID WITH ELENI MANIS, THE DIRECTOR OF RESEARCH AT THE SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT 26](#_rx18nuo9t8ip)

[A CONVERSATION I HAD WITH A MEMBER OF NYCFAR AT THE WOMEN’S STRIKE FEST 29](#_jrb5j6ob93la)

[COLLECTED MATERIALS 30](#_5vprf58e1yma)

[VIDEOS + PHOTOS 32](#_yahbz0i2mkvq)

[TIKTOKS 32](#_9qyzzj5pe0yr)

[STOP THE SCAN PRESS CONFERENCE 32](#_7mt8jwidwct9)

[LOGS 33](#_nulvcm5dj1mu)

[PROGRESS LOGS 33](#_c64k8shx9up4)

[LOG #1: KILL THE COP INSIDE YOU (2-22-23) 33](#_ngtcugi7c1x9)

[LOG #1 RATIONALE: 36](#_e0q0wed1sygi)

[LOG #2: CAMERA SMASHING (3-9-23) 37](#_qv9h0b3yiiyr)

[LOG #2 RATIONALE: 40](#_mk3c3wgpz3k)

[LOG #3: ANTI SURVEILLANCE SOCIALS 41](#_xiaihzeiia1k)

[LOG #3 RATIONALE: 43](#_66zkrtkegou7)

[LOG #4: WELCOME TO TIK TOK 44](#_o1fukyic9pnm)

[LOG #4 RATIONALE: 46](#_ms6n926molte)

[REFLECTION LOGS 47](#_xu6cslalbh7z)

[LOG #5 47](#_hq4kfi3xij74)

[LOG #6 RATIONALE: 48](#_iz2md5k1eb41)

[SUMMARY EVALUATION 49](#_dbkhrj7c4byk)

[FIRST SEMESTER PAPER AND ANNOTATED BIBLIOGRAPHY 55](#_qv3evvvczxx4)

# STATEMENT OF COURSES PARTIALLY DROPPED

None.

# FIRST SEMESTER QUESTIONS

**TOPIC QUESTION:** How does Mass Surveillance affect the state of reproductive rights post Roe and what can be done to protect them in the future?

**GUIDING QUESTIONS:**

1. What is digital surveillance?
2. What does digital surveillance look like in 21st century America?
3. How does a surveillance state threaten reproductive rights?
4. What legal limits on surveillance exist in the United States?
5. What digital information related to reproductive health does the government have access to?
6. How has digital evidence been used to prosecute abortion seekers?
7. Can abortion be truly protected anywhere in 2022?
8. How are activists fighting back against surveillance?

# FIRST-SEMESTER PAPER SYNOPSIS

For my research paper, I took a deep dive into the causes and effects of reproductive surveillance, specifically after the overturn of Roe V. Wade. I started out by explaining what surveillance is, and why pregnant people are targets for it. I defined the limits of surveillance in the US, and then I looked at different methods of surveillance, geolocation tracking, search history surveillance, license plate readers, school surveillance, etc. I examined how digital evidence collected through surveillance has been used to prosecute abortion seekers and how it could be used in the future. For the counter perspective I explained third-party doctrine and Big Tech’s response to criticisms that they aren’t doing enough to protect pregnant people digitally. Finally, I ended the paper with the efforts being made to take action against surveillance in different avenues of activism.

# FIELDWORK QUESTIONS

HUMANITIES PROJECT

1. What is reproductive health data and how is it collected and disseminated?
2. What other types of surveillance affect activist movements?
3. How much faith do activists have in corporate and legislative solutions?
4. What does surveillance disruption look like on the grassroots level?
5. How is digital self-defense information being distributed, and to what extent does it help?
6. What role can ordinary citizens play in protecting reproductive health data?
7. What does fighting surveillance on social media look like?

# FIELDWORK SITES

NOTE: I was not able to find a mentor. Instead, I had the opportunity to speak to many different experts and experience a very valuable fieldwork experience.

**Surveillance Technology Oversight Project**

Virtual

Worked with Will Owens ([William.Owen@stopspying.org](mailto:William.Owen@stopspying.org))

Met with Eleni Manis ([Eleni@stopspying.org](mailto:Eleni@stopspying.org))

Met with Leticia Murillo ([Leticia.Murillo@stopspying.org](mailto:Leticia.Murillo@stopspying.org))

I did a lot of work with STOP. I started out talking to Leticia in February about getting involved. Then I talked to research director Eleni Manis about the paper she co-wrote and how to get involved with the organization. She referred me to Will, who got me involved with STOP’s social media team.

**Meeting with Abby Abrams** (2/15 @ 4pm)

375 Amsterdam Ave, New York, NY 10024

[abigail.abrams@gmail.com](mailto:abigail.abrams@gmail.com)

Abby Abrams is a journalist who wrote a piece for TIME on surveillance conducted by anti-abortion pregnancy centers. I reached out to her and we sat down at Daily Provisions (a cafe) to talk about her piece. It was a great conversation, and my first in person fieldwork event.

**Abortion as Abolition Panel at Barnard Center for Research on Women**

(2/17)

Barnard Center for Research on Women, 6th Floor, Milstein Center, Barnard College

3009 Broadway

New York, NY 10027

I found out about this panel through New York City For Abortion’s instagram. It was a great panel, where I got to hear activists and legal defenders talk about the criminalization of self managed abortion. It was my first real foray into pro-abortion activism.

**Women’s Strike Fest** (3/11)

Washington Square Park

Met members of New York City for Abortion Rights

I found out about this event on NYCFAR’s instagram, and thought it would be a great chance to finally meet the activists I wanted to talk to. It was a great experience to see a local activist gathering, talk to clinic defenders, and collect some interesting material.

**New York City for Abortion Orientation Meeting** (2/20)

Virtual

I got the opportunity to attend an orientation for grassroots NYC clinic defense activist group NYCFAR. I got an up close look at the security of a reproductive justice group.

WORK SITES

**Dwight Englewood Imperatore Library**

315 East Palisade Avenue Englewood, NJ 07631

This is where I did prep work for my fieldwork. Sending out emails, doing research, and writing logs.

**My grandmother’s house**

300 Katherine Street, Englewood, NJ 07631

**My house**

605 West 111th Street, Apt #31, NY, NY, 10025

These two places are the two different places where I live, and it’s where I got the majority of my work done.

# HOURS PER WEEK

Fieldwork Conducted from 2/6 to 5/5 → 14 weeks

| Week | # of hours |
| --- | --- |
| 2/6 | 2.75 |
| 2/13 | 5 |
| 2/20 | 2 |
| 2/27 | 1 |
| 3/6 | 2 |
| 3/13 | 1.5 |
| 3/20-4/3 | 3 |
| 4/14 | 2 |
| 4/17 | 4 |
| 4/24 | 2 |
| 5/1 | 3 |

# FIRST SEMESTER BIBLIOGRAPHY

Alder, Steve. “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/.

Najd Alfawzan, Markus Christen, Giovanni Spitale, and Nikola Biller-andorno.

"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.

Amster, Haley, and Diehl, Brett. "Against Geofences." Stanford Law Review 74, no. 2 (2022): 385-445.https://ezproxy.d-e.org:2443/login?url=https://www.proquest.com/scholarly-journals/against-geofences/docview/2646758135/se-2?accountid=35837.

Baker-White, Emily, 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. Accessed November 1, 2022. https://www.forbes.com/sites/

emilybaker-white/2022/08/08/facebook-abortion-teen-dms/?sh=2501927a579c.

Benson, Thor. "The Danger of License Plate Readers in Post-Roe America." *WIRED*. Last modified July 7, 2022. Accessed September 20, 2022<https://www.wired.com/story/license-plate-reader-alpr-surveillance-abortion/>.

Cahn, Albert Fox, and Manis, Eleni. "Pregnancy Panopticon: Abortion Surveillance

after Roe." *S.T.O.P,* May 24, 2022, 1-16. Accessed September 19, 2022.

<https://www.stopspying.org/pregnancy-panopticon>.

Conti-Cook, Cynthia. "SURVEILLING THE DIGITAL ABORTION DIARY." *University of Baltimore Law Review*, Volume 50, 0-76.

Duhigg, Charles. "How Companies Learn Your Secrets." *New York Times Magazin*e. February 16, 2012. Accessed September 28, 2022. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

Feathers, Todd. "After Dobbs, Advocates Fear School Surveillance Tools Could Put Teens at Risk." *The Markup*, July 8, 2022. Accessed November 29, 2022. <https://themarkup.org/privacy/2022/07/08/after-dobbs-advocates-fear-school-surveillance-tools-could-put-teens-at-risk>.

Gordon, Marcy “Democrats widen scrutiny of tech over abortion data privacy.” AP News, July 22, 2022, accessed November 16, 2022, https://apnews.com/article/abortion-technology-apple-inc-congress-government-and-politics-fa6dfd46baeb3732df4b4fcb720dd04a

Hunter, Tatum. "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/.

Hunter, Tatum. “Planned Parenthood Suspends Marketing Trackers on Abortion Search Pages.” The Washington Post. WP Company, June 30, 2022. https://www.washingtonpost.com/technology/2022/06/30/planned-parenthood-privacy-data/.

Keegan, Jon and Tarr, Donna. "Online Abortion Pill Provider Hey Jane Used Tracking Tools That Sent Visitor Data to Meta, Google, and Others." The Markup, July 1, 2022. Accessed December 5, 2022.

Meta, “Correcting the Record on Meta’s Involvement in Nebraska Case”, Meta, August 9, 2022, accessed November 16, 2022, <https://about.fb.com/news/2022/08/meta-response-nebraska-abortion-case/>

Fitzpatrick, Jen, “Protecting people’s privacy on health topics.” The Keyword, July 1, 2022, <https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/>

McCubbin, Sabrina. "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>.

“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>.

Pew Research Center, “Mobile Fact Sheet,” *Pew Research Center*, April 7, 2021, <https://www.pewresearch.org/internet/fact-sheet/mobile/>.

Sisitzky, Michael and Schaefer, Ben, “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

Su, Sara, “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/>

Wiggers, Kyle, “Tech companies respond to US Supreme Court abortion decision” TechCrunch, June 24, 2022, <https://techcrunch.com/2022/06/24/tech-companies-respond-to-u-s-supreme-court-abortion-decision/>

Wylie, Christopher. *MINDF\*CK: Cambridge Analytica and the Plot to Break America*. S.l.: RANDOM HOUSE, 2019.

# SECOND SEMESTER BIBLIOGRAPHY

Abrams, Abigail, and Vera Bergengruen. “Anti-Abortion Pregnancy Centers Collect Personal Data.” Time. Time, June 22, 2022. https://time.com/6189528/anti-abortion-pregnancy-centers-collect-data-investigation/.

Adler, Natalie, Anne Rumberger, Elizabeth Narvarro, Jessie Kindig, and Marian Jones, eds. *We Organize to Change Everything: Fighting for Abortion Aces and Reproductive Justice*. New York, NY: Verso Books, 2022.

Anonymous. “Blinding the Cyclops-Wrecking the Panopticon.” CrimethInc., 2020. https://crimethinc.com/2020/07/14/blinding-the-cyclops-wrecking-the-panopticon-camera-hunting-in-the-metropolis.

Ashworth, Boone. “The NYPD Brings Robot Dogs Back.” Wired. Conde Nast, April 15, 2023. https://www.wired.com/story/nypd-spot-boston-dynamics-robot-dog/.

Borradaile, Glencora. *Defend Dissent: Digital Suppression and Cryptographic Defense of Social Movements.* 1st ed. Corvallis, OR: Oregon State University, 2021.

Kalish, Jon. 2017. “Cryptoparties Teach Attendees How to Stay Anonymous Online.” NPR. February 6, 2017. https://www.npr.org/sections/alltechconsidered/2017/02/06/513705825/cryptoparties-teach-attendees-how-to-stay-anonymous-online.

Leonard, Sarah. “The ext Abortion Strategy.” Lux Magazine, February 25, 2023. https://lux-magazine.com/article/the-next-abortion-strategy/.

‌

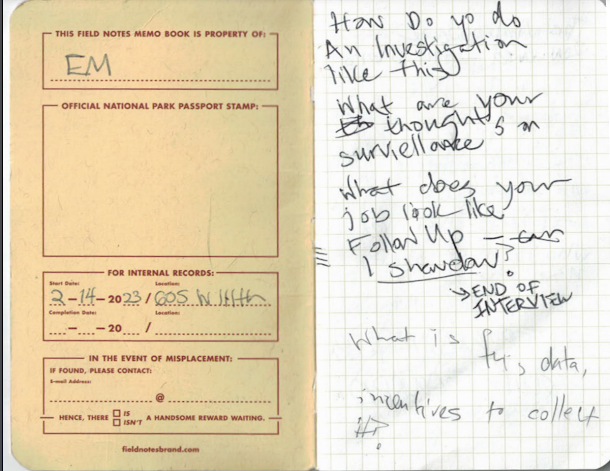
# EVIDENCE

## NOTES

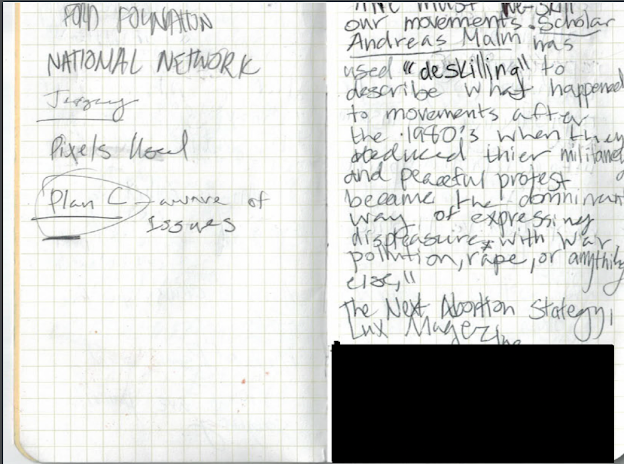
### NOTES RATIONALE

These notes were taken at various meetings I went to during my fieldwork. One set with journalist Abby Abrams, another set of notes at a Barnard panel on Abortion, and a third set from attending a NYCFAR orientation. The notes were a good way to document my findings and make sure that I had good, specific information to put in my progres logs.

### NOTES FROM TALKING TO ABBY ABRAMS

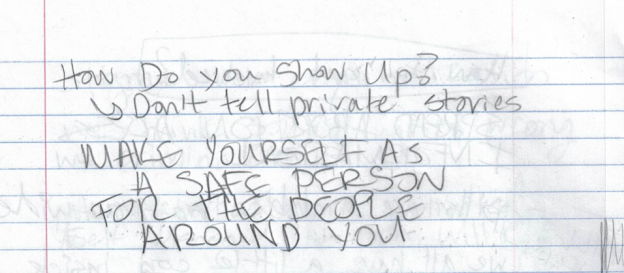


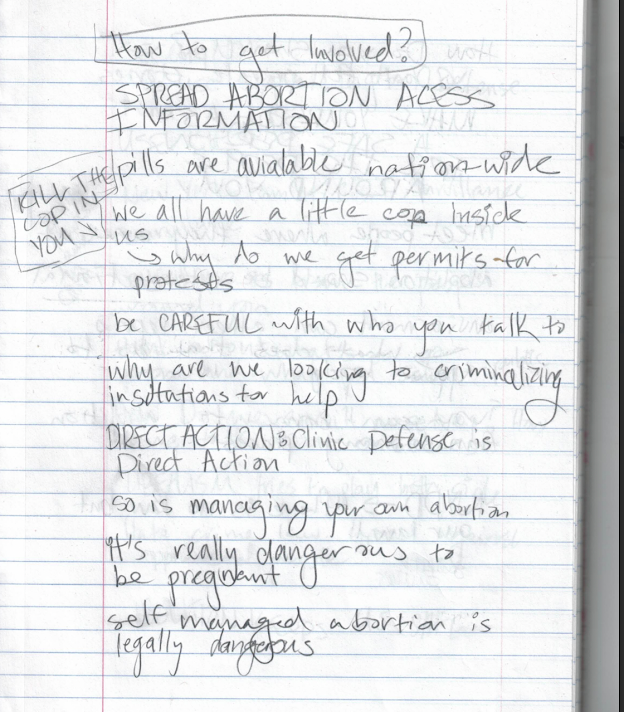




### NOTES FROM BARNARD ABORTION AS ABORTION PANEL

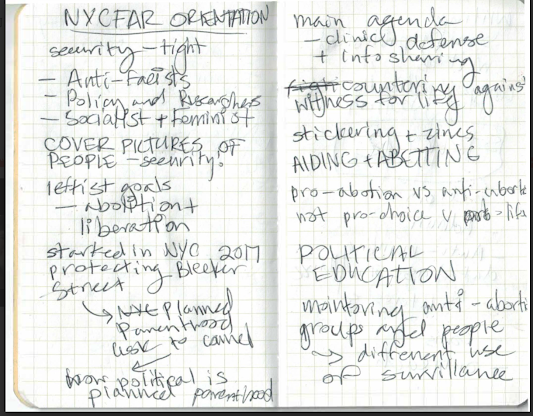
### 

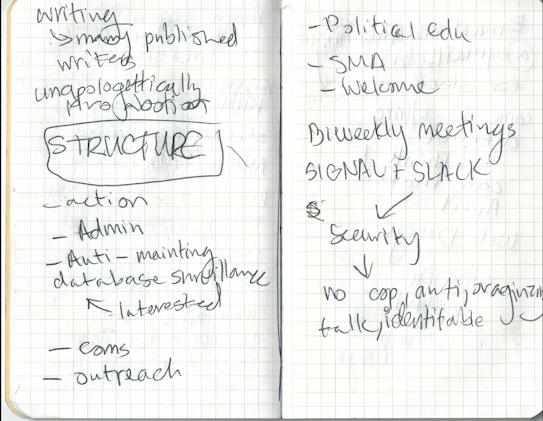


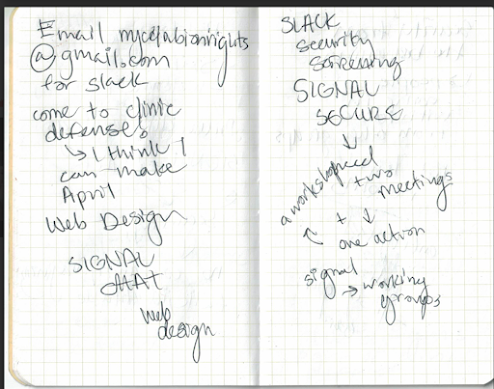


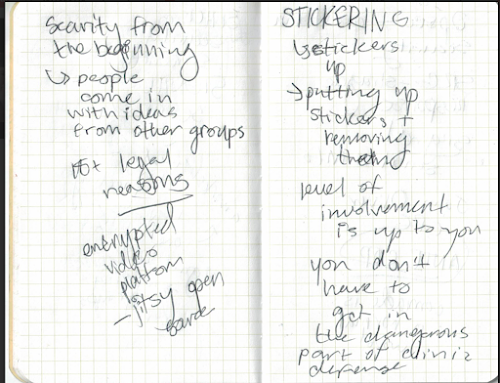


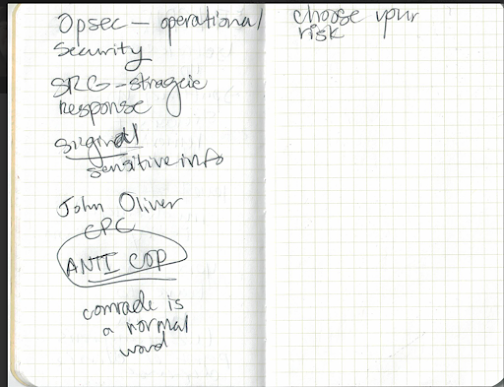
### NOTES FROM NYCFAR ORIENTATION











## TRANSCRIPTS

### TRANSCRIPTS RATIONALE

Through the second semester, I got to talk to some knowledgeable experts in my field. Abigail Abrams, a journalist covering reproductive rights in the United states, was the person I talked to. We spoke about a piece she wrote on surveillance conducted by pregnancy crisis clinics. The next person I talked to was the director of research at the Surveillance Technology Oversight Project. She co-wrote one of the center sources for my research paper, STOP’s pregnancy panopticon report. Finally I talked to a member of NYCFAR (New York City for Abortion Rights) at the women’s strike festival. These transcripts allow me to put detailed evidence of these insightful conversations into my portfolio. They were key to answering my fieldwork questions.

### 

### SNIPPET FROM A CONVERSATION WITH ABBY ABRAMS

Emma: So, How did you start looking into the surveillance done by anti-abortion centers?

Abby: I mean, the way we started looking into it was really that I had been reporting on abortion for a few years. And kept hearing from advocates that they would encounter women who had kind of been tricked or like gone to one of these centers that is not an abortion clinic and didn't realize that.

And so they would go to the centers thinking they were gonna get medical care and then realize that sometimes that they were like a more religious institution or whatever.

And so that idea of the fact that they had often filled out a full form with their medical history and information and. Like relationship history.

Emma : Yeah.

Abby: Like your sexual history, all kinds of stuff. And so we started looking at the forms that they had patients fill. Have, yeah. And a lot of them, so some of them put the forms online so you can actually look those up.

You go to like the Center's websites if you, for New York or if you wanna like see other cities, if you just Google like, you know, Austin, Texas, like pregnancy Center, if you go to their website, they'll sometimes have the form, or at least like an intake form that they would have a woman potentially fill out.

Emma: That sounds great to look into.

Abby: Yeah. And you can kind of like, See the types of questions they're asking. And they would say things that were like privacy insurances, right? Yeah. You're like, we promised that this is confidential. But that does not guarantee it, Because it's not HIPAA protected. We started looking into this. There are a lot of then nonprofits that have done their own research on this area.

So that's something, I don't know what documents you've looked at.

Emma: Not many.

Abby: We kind of worked with non-profits and then that gave us more places to dig into, And eventually we kind of created our own database of intake forms and we're able to, to look at a larger scale of what kinds of questions.

Emma: What prompted you to start looking at data specifically?

Abby: I mean, once the Supreme Court decision leaks, I think we were just thinking about ways that like current practices last spring, would it get worse or become more, you know, dangerous.

Emma: Mm-hmm.

Abby: And so that idea of the information that you're giving up suddenly being in the hands of people who like them all of a sudden have more motive to do something with this.

Emma: I've been following this surveillance, looking at geolocation tracking, Text messages, search history, all that kind of stuff. Keyword warrants, etc.

Emma: And are the people you’ve spoken to worried about this, how much awareness is there of digital surveillance when it comes to abortion?

Abby: Yeah, I think that like normal people are getting more aware but are not, I think that's part of the big problem All the experts are very worried about it, but if you're kind of a regular person who maybe doesn't even read the news accurately, you certainly know that like your state laws might have changed, but you're not thinking before you Google. Like, especially if you're in a moment where you are freaked out and help.

Emma: What would be the best way to get people more informed on this?

ABBY: A lot of groups have done good, like social media campaigns, about trying to raise awareness on the privacy front. Yeah. So I'm sure you've probably seen it on Instagram. When Roe was overturned, there were lots of people posting to be aware of privacy. And I would say that at least, like obviously the people that I know are more limited. Somewhat. t I'm from St. Louis and so I still have friends that live in Missouri. And people there that I know who like who don’t work in media or politics are at least aware that if they need to travel or do something, they should be slightly more careful. Like they should be thinking about something, but they don’t know what steps to take.

—-

Emma: These anti-abortion centers, do they have any links with Big data companies or anything like that?

Abby: Their network is a big group of pregnancy centers and they sell this project management system basically to all the different individual centers.

Emma: Yeah.

Abby: We didn't get as much into this, but, there's some, I think on their board or certainly people that they have gotten money from. There's some link to like conservative folks who have funded other kinds of data operations. And that is something potentially that other people could look more into.

I'm sure if you look up their board members. Yeah. I remember that we had to kind of slim down the investigation to focus on that legacy. You wanna, you don't wanna go crazy. But looking at any of these companies, board members and then looking at those board members, like where else they have donated money, where else they're all the board of that is like a way to do these things.

None of them are involved in, you know, it's not as though they are explicitly involved with Facebook. But they're like, I mean, I'm sure you've read about the Facebook pixels that are down, lots of clips, in that way they're Planned Parenthood. It's more that there are conservative groups that try to like, collect lots of data centers or lots of whatever websites they're using.

Emma: I think the, like, since you've covered this before and after road, do you think when it comes to data, has it changed? Because I know there were cases where people were prosecuted using digital data beforehand, right.

Abby: You know, I think we're probably still in the beginning of this, I think is the tricky part, right?

And there's like all these concerns that this data will be used in the wrong way. There was one in Nebraska. I think that probably in the next year or so I would say we know more.

Emma: There are a lot of incentives to collect this data, like in Texas. Have, is there more concern there with vigilantism, have you seen anything with that?

Abby : Yeah, so the Texas thing is really interesting cause originally there was a ton of concern about yeah, that there would be all these bounty hunters, To make use of the law and then get $10,000. And what we've seen is that there have been really almost no cases.

Emma: That’s really interesting.

Abby: And I think, so it's worked out as more of a deterrent from doing anything. So like from people breaking the law. But I would say that the kind, the incentive to reflect the data, I think would be more of an issue once we start having more laws about traveling out of the state more.

Emma: Right. And at these pregnancy centers, the databases where they keep this, is that like encrypted data?

ABBY: Where like Heartbeat International keeps all this data? It's definitely not.

EMMA: So is it like vulnerable data that anyone can get?

ABBY: Yes. So we weren't able to get the information about how they keep the data here, but we did not see any evidence that they have particularly strong IT practices. And they have not talked about, you know, levels of security that they have to protect these kinds of things. And often, the people collecting this data are unpaid volunteers. And they're totally just like either nurses or random people who have this mission.

EMMA: So not people who are necessarily adept at using secure systems.

ABBY: Yeah. Yeah. I think that's something to think about as well. The people collecting the data are not trained people.

### 

### SNIPPETS FROM AN INTERVIEW I DID WITH ELENI MANIS, THE DIRECTOR OF RESEARCH AT THE SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

EMMA: how do you start investigating a type of surveillance and you fall in?

ELENI: Okay, so the kinds of surveillance tools that we are concerned about being turned on pregnant people are the same surveillance tools that have been turned on previously overpoliced communities. So black and brown communities, especially black and brown youth immigrants, especially undocumented people, LGBTQ people protesters.

The means of surveillance are not new. The target is new which means we have a massive head start, unfortunately, on understanding how surveillance will be used against pregnant people seeking abortions.

–

EMMA I was wondering, in the, in your article, you mentioned data sharing, sharing agreements between police departments, and I was having a little trouble finding stuff on that beyond your paper, so I was wondering, could you elaborate on that?

ELENI: Okay, so fusion centers exist in every state and in many major metro areas.

They are data sharing centers where local police share data with state and federal agents and immigration agencies like ICE. I'm trying to remember what the context was for data sharing. They're both informal data sharing agreements between police agencies. They're actually centers where police agencies specifically put their data and work in collaboration with federal agencies. There's also cross state data sharing if that's what you're.

EMMA: I think the context in your article was New York sharing data with an anti abortion state that the police collected because people are starting to come here to get abortions. I think that was... That you raised. So yeah, that was, yeah, I mean, the concern is that there are very few limits on data sharing among police agencies.

And so unless you live in a sanctuary state, and police are obeying restrictions on data sharing, it’s a concern. Yeah, you may well have police helping to criminalize travelers to those states.

EMMA: STOP is working on Banning geofences in New York City, which is great. But how does that go with such a strong police department? department and it seems like surveillance is something very useful to policing. So is that something you have a lot of faith in?

ELENI: What STOP really needs is a geofence warrant ban nationally. Because it's, it's a tiny piece of the puzzle for any particular municipality to use to hand over data. And if Alabama can compel data from Google, it really doesn't need the NYPD to share data or not. Yes. Do I have faith in the ability of the New York City council to pass a bill?

Yeah, I do. I mean, we managed to pass the POST act, which requires the NYPD to publicly announce its surveillance technology. So I do think that when coalitions of interested parties get together, they can move mountains.

EMMA: Do you have a preferred avenue of change that you think works best for fighting surveillance.

ELENI: There's a federal bill, there's a city bill, there are lawsuits, there are white papers and support, you know, that start to formulate next steps for legislative work or for advocacy work. We work all angles and just wait for something for one of the levers to move.

—

ELENI: I think the next thing for you, incidentally, is to recognize how close the criminalization of gender affirming care is to the criminalization of abortion. The next thing for us is thinking about how travel across state lines could be complicated by surveillance for people who are seeking abortion outside of the states where they live where it's been criminalized, the exact same thing for parents who are traveling out of state to get their kids gender affirming care.

Same thing for anybody, honestly, who's traveling out of state to do something that they're not allowed to do in their own state. Any legitimate reasons why a person might need to, might need to leave a conservative state to, you know, pursue something out of state. But it's really striking how close the analogy is.

It's not even an analogy. These are two groups facing the same struggles.

—-----

EMMA: The digital self-defense information that STOP and other organizations release, how much does that information actually help that information has really helped people?

People seeking abortions are working in a hurry, possibly in a crisis. So to expect individuals to truly protect themselves with, you know, measures that are going to be partially successful at best is a lot to ask, which is why we spend the vast majority of our time pushing big tech and regulators to protect abortion seekers.

EMMA: Right. Because it is so difficult to travel untracked to an abortion clinic.

ELENI: That's the best way of thinking about these. You know, we want protesters, we want people seeking reproductive health care. We want undocumented people to take steps to protect themselves from undue police surveillance. But we also know that the only real solution is going to be to change the landscape of surveillance in our country.

### A CONVERSATION I HAD WITH A MEMBER OF NYCFAR AT THE WOMEN’S STRIKE FEST

EMMA: At orientation I noticed at your orientation that you guys have a very strong security system, how did you come up with that?

NYCFAR Representative: It was a group effort. After we had some issues with the police we stepped it up. Different Members brought different ideas from different groups. We also worked with the Digital Defense Fund and The Surveillance Technology Oversight Project

EMMA : Yeah I’ve been talking with them about my project.

NYCFAR Representative: Oh wow! Yeah so all the stuff you saw at orientation with the slack and the signal is a way to keep ourselves safe. Everything about the reproductive health app data surveillance is true, but it [surveillance] gets much more intense when you’re an activist.

EMMA : I know NYCFAR does monthly clinic defense, and has issues with NYPD’s SRC. How do you protect yourselves against police surveillance during that?

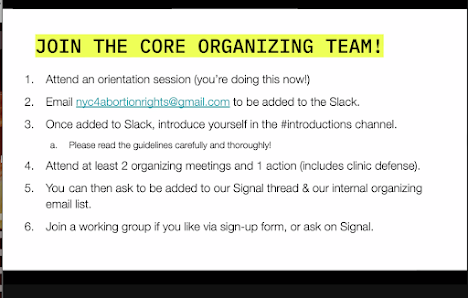
NYCFAR Rep: We wear unidentifiable clothing, cover our faces both for security and safety, we make sure to tell people to leave behind things college shirts and hats. When it comes to antis [anti-abortion supporters] we make sure to notice what they’re wearing.

EMMA: Beyond digital surveillance, how do you deal with low tech surveillance? At a panel I went to at Banard activists mentioned that when self-management is criminalized it’s because of low tech surveillance.

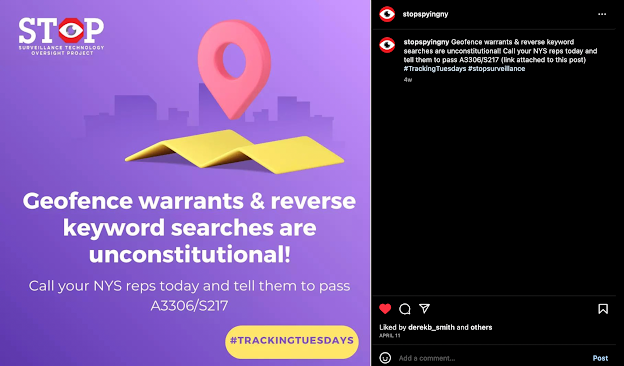
NYCFAR Rep: I don’t talk to my closest friends about this stuff. We’ve had issues in the past, and no matter how good your security system is, if you let the wrong person into it they can wreak havoc. That’s why we make it so hard to get access to our information. Some people can be more open about it than others. Like I had an abortion six years ago in New York, but other people aren’t that safe.

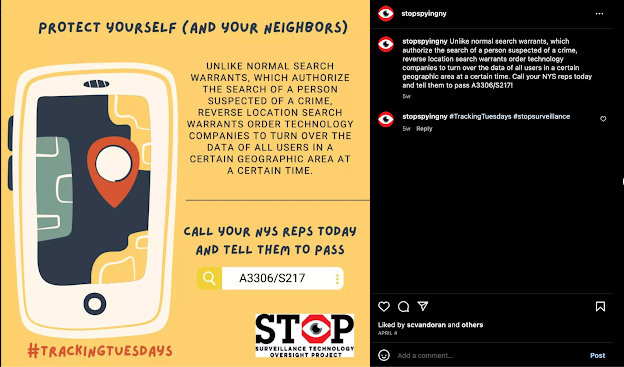
## COLLECTED MATERIALS

These are various digital materials that I’ve collected throughout my fieldwork related to advocacy and social media.



A SCREENSHOT FROM NYCFAR’S ORIENTATION





S.T.O.P. SOCIAL MEDIA POSTS



From Shout Your Abortion

## VIDEOS + PHOTOS

### TIKTOKS

As part of my fieldwork, I worked with Will Ownes at the Surveillance Technology oversight project to design some short videos for STOP’s Tiktok Page. I made three of these videos, trying out different ways of communicating the danger of geofences and the danger of abortion criminalization. One of these videos is getting published. It the best lit, and it’s the most snappy, with different layers of articles on beat with music.

[Articles.mp4](https://drive.google.com/file/d/1gCPyNBGfQ0nksfdVulHgJi1OGSPeNyBo/view?usp=share_link)

The other two ([geofence.mov](https://drive.google.com/file/d/174rqo-xeLQQU4BZsh3SZIJrNt2JcZUbL/view?usp=share_link), [duck.MOV](https://drive.google.com/file/d/10K9HFj5nJjRJ3l7WoJdGxD7BTAYyDRwv/view?usp=share_link)) needed tighter scripts.

### STOP THE SCAN PRESS CONFERENCE

I participated in one of S.T.O.P’s press conferences/ rally to ban discriminatory facial recognition, and it made the local news!



That’s me on the right, and [here is the link to the press conference.](https://www.youtube.com/watch?v=Lpi8V_3umkY)

## 

# LOGS

## PROGRESS LOGS

### LOG #1: KILL THE COP INSIDE YOU (2-22-23)

This Friday I went to a panel at Barnard called *Abortion as Abolition* where I learned about self-managed abortions. It was my introduction into grassroots organizing and activism. I got to dive deeper into pro-abortion organizing when I attended New York City for Abortion Rights (NYCFAR) orientation. The information I learned at these respective events helped me begin answering the questions I have regarding the activist side of my research.

What other types of surveillance affect activist movements?

One type of surveillance I hadn’t read much during first semester was low-tech surveillance. One of the people on the Barnard panel was a legal director for If/When/How, a legal reproductive advocacy group, said that while digital surveillance does play into the criminalization of self-managed abortion, in the cases they looked at it was individual people reporting abortion seekers, not geofence warrants. The activists cast a wide net to define cop. This new definition includes prosecutors, judges, CPS, social workers, state physicists and psychologists, and in some cases, mandated reporters like teachers. In this definition “cop” is anyone who has to report to the police. I’m not sure how I feel about this.

I am curious about the issue of paranoia. In the state of our country it’s important to be careful, but I do wonder if seeing so many people around us as agents of surveillance is a good idea. Activists are very for community building (a “we protect us” mentality). Does a fear of being surveilled by the people around you conflict with that? There are a lot of balancing acts when it comes to dealing with surveillance, and I can see where it gets difficult to navigate.

This panel also helped me better understand the goals of the grassroots movement for reproductive justice.

NYCFAR, a grassroots organization, is one on the left. They identify as anti-facist, feminist, socialist, and abolitionist (as in abolition of the police). They follow a framework of reproductive justice: The right to have a child, the right to not have a child, the right to raise that child and the right to bodily autonomy. They identify as pro-abortion rather than pro-choice because not all women with the “choice” (ex. Living in NY) doesn't necessarily mean someone has access to abortion. They unabashedly use the word abortion. (--> Shout Your Abortion organization).

What does surveillance disruption look like on the grassroots level?

NYCFAR has an incredibly well thought out security plan. To get into the password-protected zoom meeting, I had to fill out a survey so they could verify that I wasn’t an anti (anti-abortion). After orientation, I was able to get onto NYCFAR’s slack, a digital chatroom. The platform is not encrypted, so the rules of communication were very strict. No last names, no ages, no locations, no cop talk, no talk of antis etc. To get into NYCFAR’s encrypted signal (18+ for legal reasons) members have to attend two meetings and one action event (a clinic defense or a workshop). Meetings are hosted on Jitsty, an anonymous open source encrypted video call platform that does not require sign ups. They have clearly put serious thought into their security because of the danger they are in. The issues seen with Planned Parenthood’s cybersecurity (the trackers on their page) might be there because they haven’t been at the same kind of risk level as NYCFAR. (This is a tentative suggestion, not a conclusion) That’s the same reason why I won’t be allowed to join their Signal (the network where real action is planned) until I’m 18.

What role can ordinary citizens play in protecting reproductive health data?

A rather bold answer to my question: Kill the cop inside you. We are all a little police officer inside us, leading us towards those biases. Activists are focusing on community support rather than police criminalization. One of the best ways to protect the people around us in a time of surveillance is to become safe to talk to. Making an effort to not share people’s personal information makes you a safer person to talk to.

Question 7: Do abortion providers and activists disagree on action taken?

There’s an argument about clinic defense NYCFAR mentioned that I have to look into, but I get the sense that activist tactics are not wholly agreed on.

Question 8: How is digital self-defense information being distributed, and to what extent does it help?

I didn’t get too much information on it specifically, but digital self-defense is something that ties together with self managed abortion. It’s essential to staying safe. NYCFAR spreads Information about SMA through zines, workshops, and social media posts.

Question 5: How do activists balance security against visibility?

This is something I’ve read about that can become a big issue in operational security. Too much security and no one knows about the movement, stopping its growth. Not enough security and outside agents can take it down all together. NYCFAR’s model takes this into account. They advertise orientations (easy to get into) on their instagram but to get access to their Signal (where all confidential information is store) you need to be more involved with the organization.

### LOG #1 RATIONALE:

In my first semester research, I was mostly looking at information coming from legal experts. This panel was my chance to look at the radical activist side of reproductive justice and anti-surveillance work I hadn’t seen before. The people on the panel were grassroots organizers, and abolitionists. After that I went to an orientation for a socialist feminist collective. They had really interesting perspectives, But I want to address some of the language they use.

The phrase “KILL THE COP INSIDE YOU” could allude to the murder of police officers, and is a very provocative phrase. The panelists were not advocating for the murder of cops, but they did believe in an abolition of the police. Using this kind of language is a debate I’ve seen played out.

For example, my mom advocates for gun control, but she calls it “gun safety legislation” because provocation can hurt a movement. On the other hand, it can be just what a situation needs. What I took out of the statement “kill the cop inside you” was a strong way of saying “don’t become part of the surveillance machine.” Radical groups prefer blunt language. Rather than referring to themselves as “pro-choice” and their opponents as “pro-life” they call themselves “pro-abortion,” and their opponents, “anti-abortion,”. The transparency of this language is something I appreciate.

These two events gave me a great look into what surveillance disruption looks like. It was here that I was reminded of the very real threat low-tech, human surveillance posed to activists, and I was able to follow up on that in another meeting with NYCFAR. Radical groups were the right people to turn to, because they bear the brunt of surveillance. They are the people out in the streets defending clinics. NYCFAR gave me a first hand look at what surveillance culture looks like: how new members are screened and how secrets are protected.

Some of the questions I was exploring in this piece lost traction as my fieldwork continued. I dropped the question, “How do activists balance security and visibility.” Because I didn’t have too many people talking to me about it. It seems like there has to be a happy middle. Too much security and a movement doesn’t grow. Too much visibility and a movement can be infiltrated and brought down.

### LOG #2: CAMERA SMASHING (3-9-23)

Camera Smashing (metaphorically and literally)

Welcome back to progress! After a weeklong-break from the concept progress - here it is:

**What is reproductive health data and how is it collected and disseminated?**

I got some more info on the question in a meeting with Eleni Manis, the director of research at S.T.O.P. One thing I’ve been wondering about since I read her *Pregnancy Panopticon* report was data-sharing between police departments. Today I was able to ask her about it. Data sharing between agencies happens in fusion centers.

Homeland Security describes them as, “Fusion Centers are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between State, Local, Tribal and Territorial (SLTT), federal and private sector partners.”

I see where the abortion concern is. Pro-abortion states sharing data with anti-abortion states (one one hand, I’m hesitant to believe pro-abortion politicians would agree to that, on the other NYPD’s SRG is basically collaborating with anti-abortion harassers.) The larger point is that law enforcement is generally free to do as it wishes when it comes to gathering data. That’s why S.T.O.P wants a ban on geofence warrants nationwide.

**How is digital self-defense information being distributed, and to what extent does it help?**

Another question I got to ask today! S.T.O.P isn’t as focused on digital self-defense. Manis considers it unrealistic to ask abortion seekers (often in crisis) to engage in inconvenient methods of avoiding surveillance that aren’t guaranteed to fully work. When it comes to digital security and security culture, the running theme seems to be harm reduction. What we really need is a strong anti-surveillance policy. If that’s attainable is another question entirely.

Grassroots activists will never have the technological power of the police-state, but they can make surveillance difficult.

Still, security methods are recommended. Manis included a section on it at the end of her paper and pro-abortion activists I speak to sing Signal’s praises.

**How much faith do activists have in corporate and legislative solutions?**

S.T.O.P uses a blunt force technique: working against surveillance in every avenue. Progress happens slowly and unexpectedly. In New York City’s council, S.T.O.P successfully helped pass the P.O.S.T act which requires the NYPD to be transparent about their surveillance (Note to self: Look into this). Right now they’re pushing for a city-wide ban of geofence warrants. There has also been success with lawsuits (gotta talk to the legal director on this, might see if I can get a hold of him.)

**What does surveillance disruption look like on the grassroots level?**

Manis trained activists in digital surveillance during BLM and the basic idea is to be careful of who holds your data (corporations + law enforcements) and find better ways to protect it.

Something that has stuck with me since we talked is what Manis said when I asked her how she led the investigation in the surveillance of pregnant people.

Simple. The surveillance isn’t new. The methods being used to surveil pregnant people today are the same methods used to surveil black and brown communities, the same methods used to surveil undocumented immigrants, and the same methods Manis fears will be used to prosecute those seeking gender-affirming care.

There is a silver lining to that. Reproductive Justice activists are not starting from scratch. There are strategies created by communities who have faced surveillance for a long time that repro justice activists can adopt. In her paper on abortion surveillance, Cynthia Conti-Cook points to the POWER NOT PARANOIA framework created by the Stop LAPD spying coalition. The Electronic Frontier Foundation published [this comic](https://www.eff.org/deeplinks/2023/02/coded-resistance-comic) on black resistance to surveillance, dating all the way back to the days of slavery (Highly recommend it, a very interesting and inspiring read). Surveillance disruption is nothing new, and it is not something reproductive justice activists are standing alone in.

On Camera Smashing

The titular topic! I recently read a zine about an anonymous writer’s adventures smashing security cameras, *Blinding the Cyclops, Wrecking the Panopticon*. Obviously, this is an illegal act of destruction, but so is getting an abortion in plenty of states. It's been an effective strategy used by protestors in Hong-Kong. Personally, this is not the first solution I’d advocate to solve the surveillance problem. Beyond the legal danger, Camera smashing seems ineffective with the sheer number of surveillance tools being used.

What I am interested in is the mentality behind it. Before they began destroying cameras, the writer felt nervous around them. Afterward, they felt empowered.

“I mean rather than our freedom of movement, our freedom to express ourselves by acting upon the world, our very autonomy—these are greatly curtailed. Our minds adjust to these new limited sets of options: employment, charity, starvation; or buy, rent, be homeless; or be observed, hide away, comply and be ignored.

But sometimes our minds and bodies remember that there was once another set of options: self-defense, attack, destroy. And it was in these options that I found dignity. When I act for the cameras now, my smile is genuine, not forced. I know I will be back to destroy them.”

This “other set of options” is a bold one, but I think it’s important to consider. We shouldn’t tolerate surveillance and the destruction of bodily autonomy. A declawed movement is what got us to where we are. There’s a difference between dissent and disobedience. And there’s a middle ground between violent anarchism and dissenting only as far as the state is willing to tolerate.

As Sarah Lenoard writes in *The Next Abortion Strategy,*

“In a best case scenario, this legal loss can galvanize a new fight. (See: Kansas voters’ resounding rejection of an anti-abortion state constitutional amendment.)

As we enter that fight, we must re-skill our movements. Scholar Andreas Malm has used “deskilling” to describe what happened to movements after the 1980s when they reduced their militancy, and peaceful protest became the dominant way of expressing displeasure with war, pollution, rape, or anything else. We will have to take care of abortions ourselves, and seize our own human rights. As we explore below and in several pieces in this issue, we need to re-learn how to perform abortions, how to support one another in getting them, how to make the lives of pro-life politicians and prosecutors hell, and how to organize local power. We cannot wait for the foundations and the national politicians to do it for us.”

### LOG #2 RATIONALE:

This log was written a couple weeks after my first one, and I think it’s where I began analyzing the more ideas I was discovering. They pushed my project in ways I did not expect.

Something Manis told me, that the surveillance doesn’t change, only the victims, is something that really stuck with me as I continued my project. It’s something I read about in Cynthia Conti-Cook’s paper in the first semester, but I began to understand it in practical terms.

While one of my fieldwork questions is “How is surveillance disrupted on a grassroots level?” The question is akin to a research paper topic question. Most of my questions come back to that general one. For a while I had thought of reproductive surveillance as a field with little research. But that’s not true. You can find surveillance disruption all across history, conducted by many groups of marginalized people. That history does not exist in a vacuum. It’s the same situation as women who are not activists panicking after Roe about what to do. The answers have lied in grassroots organizing for years, we just have to look for them.

I was reminded of this two months later, when I went to a S.T.O.P rally on banning discriminatory facial recognition technology. None of it related to abortion defense directly, but all of it was applicable. Collaboration with city counselors, learning how a press conference works, watching activists interact with each other, working to ban technology that has become another way of surveilling marginalized people, and could become a way of targeting abortion seekers.

Intersectionality was something I was aware of, but I have finally realized just how important and specific it is to my field of research.

### LOG #3: ANTI SURVEILLANCE SOCIALS

4-14-23

**What does fighting surveillance on social media look like?**

To prepare to work with S.T.O.P social media time, I’ve done some research on anti-surveillance social media posts to try and figure out what does and does not work.

#TrackingTuesdays: A hashtag STOP posts to every Tuesday, with information about how to help their work. Colorful graphics with phone numbers for New York Representatives and the number of their bills.

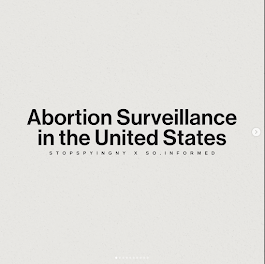
They have similar info on their Twitter. Information on online events, bills, and news about what the NYPD is doing with surveillance. They share work other organizers are doing. It’s a good stream of information for people who want it. The graphics are colorful and inviting, but they don’t have very much activity. Their account has 13k followers on twitter. However, even there, with over ten thousand followers, they don’t have very much engagement.

For example this post, an invitation to an event:

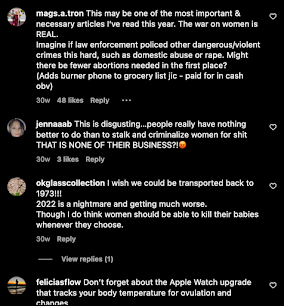
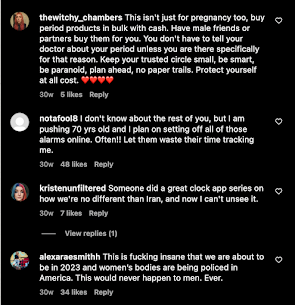


Seems very inviting to me. The information is clear, the colors are nicely contrasted, and the illustrations grab my attention. However, it has three likes and 0 comments, which feels disproportionate to their audience.

In contrast this post, a collaboration between S.T.O.P and so.informed, an minimalistic informational account with three million followers, has 137 comments. (I was unable to see the number of likes) It’s specifically on the topic of abortion surveillance.



The post isn’t something I’d expect to blow up on social media - it’s about 10 slides of well researched information on a white background. It’s hard to say why it blew up. I’d give a couple of guesses: So.Informed already had a large base of followers, the format worked very well, and it was posted a month after Roe vs. Wade was overturned. And not only was it popular, but people genuinely responded to it. Here are a couple of comments:



From this handful of comments, there is real and palpable rage. If you can get their attention on social media, people act in accordance. The next step is getting them in the streets.

Evidently, getting people engaged when it comes to activism can be a random and frustrating process. But as we’ve seen over the past couple of years, success on social media can make a movement grow exponentially.

### LOG #3 RATIONALE:

This log is a quick deep dive into the world of social media. These are only two data points, and I don’t want to make any sweeping conclusions. Looking into social media was something I started later in the process, and it’s been very interesting. In my research, I came across a lot of information on how social media allows for an incredible amount of surveillance, and I think that turned me off using it as a source. But in the past few weeks I’ve learned things are more complicated than that.

Social media is an essential part of activism today. That is a big generalization, but it’s one most people would agree with. That means even when it comes to causes that go against social media’s ideology, like fighting surveillance, it’s still important to use it.

This comes back to a question about surveillance and I decided to get rid of: How do activists balance security and visibility? Social media is a massive component of visibility. It’s part of mobilization. This log looks at two different types of posts and how people respond, and that is very important information to have. Part of my research has included looking through activist accounts, but it was great to have the time to actually analyze them.

### LOG #4: WELCOME TO TIK TOK

4-21-23

What does fighting surveillance on social media look like?

I got to learn about this firsthand this week! Since STOP has a pretty dead TikTok, so I was asked to make some for them.

One of the ways STOP fights surveillance is through local legislation, and right now they’re lobbying for a bill to ban reverse search warrants (keyword and geofence) in the state of New York. Their angle on social media is to keep asking people to call their representatives and be aware of what the bill is.

The angle I took with it was to try and explain what a Geofence warrant actually is. When I started learning about them they were hard to wrap my head around, and when I was talking to other people about my paper, they also had some trouble understanding it. Hopefully, if more people understand geofence warrants they’d want to support this bill. What I tried to do this week was record a one-minute video explaining what exactly a geofence is, and why they create privacy issues.

I’m meeting with Will (communications director) to show him what I’ve made on Tuesday. I’m going to keep going with the whole explanation of what geofence warrants are and get a few different videos.

It is interesting an interesting situation to be in, campaigning for privacy protections using apps by companies making the problem worse. Obviously, it’s the way to reach people, but it’s something to think about.

Social media, specifically Tik Tok, is tricky because you have to grab people’s attention and explain complex subjects in short and easy ways. I’ve read a 40-page legal article on Geofence Warrants, and now I have to get the bare bones in a quick addictive way. Before this I didn’t realize how tricky it is to communicate ideas on social media.

What I’m trying is to make videos snappy (lots of cuts) or weird enough to sustain interest (film with a goose lamp). After scrolling on social media for even a little bit, I remember nothing, so the goal would be to make someone switch apps and google something.

Social media is a gateway to activism. It’s how I found some of the groups I talked to, it’s how protests are advertised, it's part of community building. There is the danger of falling into armchair activism (saying things online and doing nothing) but what S.T.O.P does (and what I’m trying to do) is get people from social media into action.

### LOG #4 RATIONALE:

In seeking to answer the question: How is surveillance fought on social media? I got the chance to try it out myself. I filmed TikToks! This was a great experience. One that allowed me to try different things, and see what I liked and what I didn’t like. There’s definitely a deeper level of learning that comes with hands-on work. So much of activism is communication: how can you effectively send a message? I was able to write a complex 18 page paper on my topic, but most people aren’t going to sit down and read that. The unique challenge is shortening it down to less than a minute. Like I said in my last rationale, doing it myself really gave me respect for the intention it takes to make posts.

It also got me thinking about something else important. Every type of social media is a different media and requires a different approach. What works on twitter (text) might not work on TikTok (audio visual). This makes social media a harder job, but a very interesting one.

### 

## REFLECTION LOGS

### LOG #5

FIRST INTERVIEW

2-15-23

I had my first interview yesterday! It was at Daily Provisions on 78th street. A crowded cafe that gave me a cup of scalding hot apple cider and all I had to go off was a picture. Yet, it all worked out. I found Abby, and we even got a table. I had a lot of nerves going into it, but as we kept talking I realized it was actually going well. I had questions and I wasn’t stuttering or laying on the verbal filler. I got different leads on anti-abortion centers in data, some good advice on fieldwork, and a whole sheet of organizations to look into. Information wise this conversation didn’t blow my mind, but it made me feel a lot more confident about fieldwork. Interviews feel a lot less scary now, and it’s great to know I can come off as professional. It makes emails a little less intimidating. I also was able to be assertive when it comes to the stage crew, and made sure I was able to go to a cool panel tomorrow. Dead-end on the mentor trail, Iz is too busy. The mentor search is proving difficult. Iz is too busy and the person she recommended is into design, which isn’t exactly my category of interest. Anyway, this whole project is really pushing me but the results are proving interesting.

### LOG #6 RATIONALE:

This log still makes me grin when I look at it. Fieldwork was very difficult for me when I began the process back in January. I couldn’t find a mentor, it felt like everyone but me had a defined path, and emails were terrifying. At one point I went to my advisor with genuine concerns I would fail the semester. I was struggling with balancing my extracurriculars with my fieldwork and was frozen at the idea of negotiating them. Finally I got an email back, with an invitation to sit down for coffee and chat. This was my first taste of victory. I was practically shaking with nervousness walking downtown. I honestly didn’t know if I could do it. Then I did.

That’s not to say this one win solved all my problems. I continued to struggle with social anxiety and my commitment to the stage crew all throughout the process.

What made this moment important was the confirmation that I was capable enough to succeed at fieldwork. Going forward, even when I felt stressed out of my mind, I grew less uncertain in my own ability. I also think it’s important to acknowledge that despite the rigor, fieldwork can be so fun and exciting.

## 

# SUMMARY EVALUATION

**What is reproductive health data and how is it collected and disseminated?**

Reproductive health data includes information given to health providers, geolocation data, health app data, data collected by license plate trackers, data from customer service tracking systems from stores like Target and Walmart, search history from phones and computers, and text messages. The collection and analysis of this data is published in academic papers I used in my first semester paper.

Geolocation data is collected from social media, and can be disseminated in the form of geofences, which is a collection of geolocation data at a certain time in a certain place. The police can obtain that information with a geofence warrant, a type of digital search warrant. Another type of location tracking comes in the form of license plate trackers. These companies can track your location by analyzing photos of your license plate. On top of that, the companies that make those cameras frequently collaborate with the police.

Health app data refers to apps like period trackers. The privacy issues with these apps hit the news pretty quickly after Roe was overturned. They have poor privacy policy and menstrual data could be used to identify a pregnancy, which could flag pregnant people seeking abortions.

Customer Service data comes from information corporations collect from their customers. An example of that is a target running an algorithm that can estimate the likelihood of pregnancy to send out ads. Pregnant people are a profit gold mine, and companies are all too willing to use surveillance to increase sales.

Search histories and text messages are some of the most personal pieces of information on our phones, and they are rarely private. Due to a lack of encryption, it’s easy for the police to gain access to them.

Information given to providers is one type of reproductive health data that has actual protection. Under HIPAA, providers have to keep that information private. However, Crisis Pregnancy Centers, anti-abortion centers that frequently pose as medical clinics, are not considered HIPAA entities. They collect the data of vulnerable people seeking help, sometimes thinking they are at a legitimate abortion clinic, with no restrictions. Abby Abrams did an investigation into this, and I was able to talk to her about it. She told me that CPCs use the same databases, and those databases do not have sufficient cybersecurity. The data is vulnerable, and patients are not protected by HIPPA.

**What other types of surveillance affect activist movements?**

Technological surveillance is relatively new, but general surveillance is not. People have been engaging in surveillance for centuries. No matter how good a digital security system is, letting the wrong person have access to it can have devastating consequences.

At Barnard Panel, *Abortion as Abolition,* the legal director of If/Then/How said that in most cases where self-managed abortions were brought to court, it was because they were reported to law enforcement by civilians, not state surveillance .

An activist at NYCFAR, a clinic defense group that has regular issues with the NYPD, told me that many activists don’t tell their closest friends about the work they do because of the issues they’ve had in the past. All it takes is one person leaking information, and an operation can fall apart. That’s why the police put in the effort to infiltrate activist organizations with the goal of collecting data.

**How much faith do activists have in corporate and legislative solutions?**

It depends on the activist. Elizabeth Warren is pushing to regulate corporate collection of reproductive health data in the senate. She believes in the work she’s doing, but She’s working within the system, not against it. She’s pushing for the protection of this data without legal threat, and she is in a position to improve the system she works under.

In contrast, when NYCFAR faces police brutality from NYPD’s SRG I’d imagine they lose faith in institutions. Some of their members talked at the Barnard, and the “we protect us” rhetoric was very strong. The emphasis was not on working with institutions, it was on building community to sustain resistance. That’s not to say NYCFAR rejects local politics. They successfully helped to advocate for a bill getting abortion pills in New York State Universities, and fight the bad police practice at city council hearings.

Eleni Manis at the surveillance technology oversight project gave me a very interesting response when I asked her the question. She said S.T.O.P. used a “blunt force” technique. They do work in litigation, legislation, and advocacy, and then see what sticks.

It’s important to note that activists have had success in the -corporate and legislative fields. Google union members convinced google to delete geolocation data around abortion clinics, and just recently S.T.O.P passed the POST act in the New York City council, which forces the NYPD to be transparent in their policing. There hasn’t been success on the national level, but activists have made strides in their local communities.

**What does surveillance disruption look like on the grassroots level?**

When working at the grassroots level, a good security system is essential. I experienced one first hand when I went to a NYCFAR training. A good system allows for new members to get involved without revealing important secrets. To get access to their Signal, an encrypted communication platform, members need to attend two direct action events.

Encrypted Communication is very important. Activists use Signal, an encrypted communication app with privacy in its core mission. Video calls to organize are held on encrypted video chatting sites like Jitsi.

At public events, it’s important for activists to make themselves harder to surveil. That means non-descript clothing, and a mask (though facial recognition is jumping that hurdle).As a general safety rule, grassroots organizations must use cation: if information does not need to be collected, it should not be collected.

On the community level, activists and technologists have hosted events called cryptoparties, where they teach people about cybersecurity. It’s important not to spread fear, but usable tools. The LA Stop Spying Coalition uses a “Power Not Paranoia” framework when it comes to fighting surveillance. Paranoia turns people on each other, which can rot an organization from the inside out. Secret keeping requires trust, and at the personal level, using passwords and not sharing digital data is important to stopping surveillance.

Especially when it comes to the illegal destruction of property, one very radical way to fight surveillance. Across the world, smashing security cameras was a way to keep themselves safe from surveillance. It’s destructive, but it works. It’s not an approach any activist I’ve talked to has mentioned, but it is worth mentioning.

**How is digital self-defense information being distributed, and to what extent does it help?**

It’s easier than ever to spread this information. Flyers, social media posts, websites, zines, word-of-mouth. Information can come from non-profits, from activists, technologists, hobbyists. There are some sites that specialize in digital self defense when seeking abortions, like the Digital Defense Fund, an organization many people referred me to.

However, the best thing this information can accomplish is harm reduction. It’s not fear-mongering to say that surveillance powers are too strong to be stopped by changing the privacy settings on your cell phone. To ask that abortion seekers, people in crisis, do all this work for a scrap of protection should not be the solution.

What we really need is legislation that protects us from surveillance. HIPAA, a law established in the 1990’s, needs an update so it can fulfill its purpose of protecting health data. On the federal level, the US needs national laws that stop companies from engaging in mass surveillance and law enforcement from taking advantage of that data.

With that far off, the next best step is passing anti-surveillance legislation in our communities.

**What does fighting surveillance on social media look like?**

The goal of fighting surveillance on social media is to catch people’s attention and get them off their phones and involved. Information needs to be spread in an interesting and quick way. Each major social media platform (Twitter, Tik Tok, Instagram) requires a different type of content. Polished infographics work on instagram, short text works on twitter, and snappy audio-visual works on Tiktok.

In all formats, complex information needed to be synthesized into a short format. Content should be regular, S.T.O.P tries to achieve this with #TrackingTuesdays. Content should also have action steps to take after watching. I had direct experience with this when I made some Tik Toks for S.T.O.P. It takes work, and I had more success using pre-existing Tik Tok sounds and trends than just talking into my phone.

**What role can ordinary citizens play in protecting reproductive health data?**

There are many ways non-activists can help protect abortion seekers from surveillance.

Politically, people can find and vote for pro-abortion and anti-surveillance representatives at all legislative levels. They can also push local representatives to support anti-surveillance bills, protect abortion, and regulate corporate surveillance. getting involved with activists fighting surveillance (either monetarily or through volunteering),

In their communities, people can support activist efforts either monetarily, or through volunteering. THey can spread information about surveillance and normalize the use of encrypted communications.

On the low-tech end, everyone has the ability to become more trustworthy, to “kill the cop inside you”, and become safe people to come to with secrets like abortions.

This country needs federal protection for abortion and consumer data. In the meantime, there is work to do.

**PERSONAL GROWTH**

I have spent this semester locked out of my comfort zone, and that has been various levels of terrifying. I really did not anticipate having that much social anxiety. When I started out, it could take me three hours to work up the nerve to send an email. Walking to my first interview, I genuinely wasn’t sure if I could handle it.

Turns out, I can handle much more than I think. I have attended panels, zoom calls, festivals, and even been in a press conference. The fear didn’t go away, I just got better at dealing with it. Everytime I overcame something hard I got more confident that the next time I ran into a roadblock I’d be able to overcome it. That confidence has allowed me to push for opportunities I want (like working with S.T.O.P on their social media team) in ways I couldn’t in January.

I’ve also had to become more assertive with the people around me in order to get my fieldwork done. One of my biggest obstacles was my commitment to stage crew, an activity that can sometimes run 50 hours per week. Even in the middle of the show, I had to learn to step back and miss a friday night to attend a meeting. Forcing myself into confrontations got me more comfortable with them. I’ve been thinking more about what I want to do, and what I need to do to get myself there.

I titled one of my recent reflections, “Growth through gritted teeth” and that about sums it up. Hard, but wholly worthwhile.

# FIRST SEMESTER PAPER AND ANNOTATED BIBLIOGRAPHY

**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.

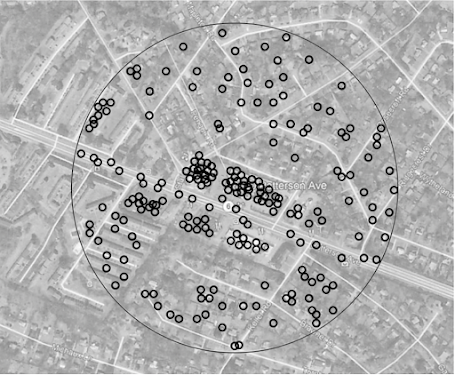
Consumer data protections on the local level can cover some of HIPAA’s blind spots. California, Colorado, Connecticut, Utah and Virginia all have consumer data protection laws in place.[[12]](#footnote-11) They give consumers the right to access the data corporations collect and opt-out of their information 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)

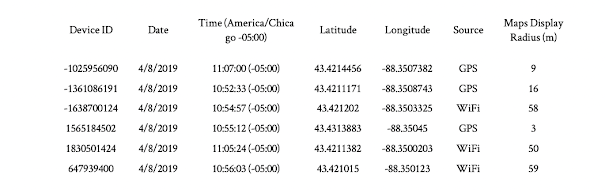
The Carpenter ruling is a new one, and courts are still figuring out how to address it. As Amster and Diel write in the Stanford Law Review, “One prominent unanswered question in this inquiry is whether the government can avoid Carpenter's warrant requirement by using many small intrusions over a large 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)

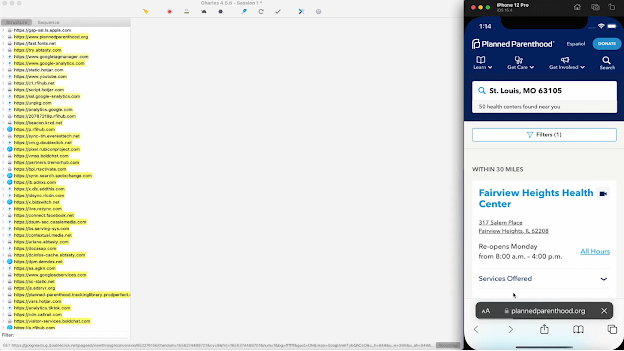
Individuals' search history can be subpoenaed along with mass groups of people’s search history through keyword warrants. Police could issue a keyword warrant on “abortion” casting a digital dragnet across the internet that would identify abortion seekers. Just like Geofences, Keyword warrants find evidence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

Alder, Steve. “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/.

This article was written by Steve Alder, the editor-in-chief of the HIPAA Journal. He has spent years researching and writing about HIPAA. The HIPAA journal has been helping major news sources and health care experts understand HIPAA. Using the Health Insurance Portability and Information Act as a source, Alder explains what Protected Health information is, what is and isn’t considered PHI, and the level of protection HIPAA offers. This source was useful to me as it explained what health information can be surveilled and what types can’t.

Najd Alfawzan, Markus Christen, Giovanni Spitale, and Nikola Biller-andorno.

"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.

This is the first major quantitative study I’ve found. in my research. It evaluates privacy policies in women’s health apps and provides specific criteria on how to evaluate data sharing privacy policies and data transparency in apps. The methodology used in the reports for determining what apps to use was based on two past studies on privacy policy and the apps evaluated were chosen using an adapted method from experts, and some of it is based on hard numbers, like downloads and reviews. It was a very useful source because it allowed me to find quantitative data on privacy and get used to reading quantitative papers.

Amster, Haley, and Diehl, Brett. "Against Geofences." Stanford Law Review 74, no. 2 (2022): 385-445.https://ezproxy.d-e.org:2443/login?url=https://www.proquest.com/scholarly-journals/against-geofences/docview/2646758135/se-2?accountid=35837.

This journal was written by Haley Amster, a law clerk at Covington & Burling LLP and Brett Diehl is a trial attorney at Federal Defenders of San Diego. The paper tackles the constitutionality of geofences. The paper covers what geofences are in depth, something that helped me understand one of the biggest forms of surveillance in a post-Roe. The article explains Carpenter v. United States and where geofences fit into it. The paper ultimately argues against geofence warrants and third-party doctrine.

Baker-White, Emily, 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. Accessed November 1, 2022. https://www.forbes.com/sites/

emilybaker-white/2022/08/08/facebook-abortion-teen-dms/?sh=2501927a579c.

This article was written by two technological journalists about a case in which a teenager in Nebraska was found guilty for murder via abortion with instant messages. The writers use police reports as evidence. This source helped me find an example legal precedent for the ideas I’m researching.

Benson, Thor. "The Danger of License Plate Readers in Post-Roe America." *WIRED*. Last modified July 7, 2022. Accessed September 20, 2022<https://www.wired.com/story/license-plate-reader-alpr-surveillance-abortion/>.

Thor Benson is an independent journalist who has written for several publications (WIRED, The Atlantic, Vice and more) who specializes in Technology. This article explains what ALPR’s are, where the data goes, and how they pose a threat to abortion seekers. From this source I understood the specifics of a type of surveillance, how it relates to my topic, and further understood the connection between corporate and governmental surveillance. Benson uses quotes from security experts, and statements from the companies he investigates.

Cahn, Albert Fox, and Manis, Eleni. "Pregnancy Panopticon: Abortion Surveillance

after Roe." *S.T.O.P,* May 24, 2022, 1-16. Accessed September 19, 2022.

<https://www.stopspying.org/pregnancy-panopticon>.

This is one of the most comprehensive reports on reproductive surveillance. It covers both private surveillance and governmental surveillance, legal precedent, privacy practices for pregnant people. Cahn and Manis use legal precedent, cited papers, personal expertise from their work, current events, and reports to paint a picture of digital surveillance both during and post-Roe v. Wade. This source provides me with both general information on surveillance and specific examples.

Conti-Cook, Cynthia. "SURVEILLING THE DIGITAL ABORTION DIARY." *University of Baltimore Law Review*, Volume 50, 0-76.

Cynthia Conti-Cook is a civil rights lawyer and technology fellow at the ford foundation, with a strong background in law and digital surveillance. Conti-Cook chronicles the legal precedent of digital evidence in prosecuting abortion seekers. She uses her expertise as a civil rights lawyer along with legal precedent to illustrate how even before Roe, digital surveillance was used against pregnant people in anti-abortion states.

Duhigg, Charles. "How Companies Learn Your Secrets." *New York Times Magazin*e. February 16, 2012. Accessed September 28, 2022. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

Charles Duhigg is a Pulitzer prize winning journalist and author who worked at the New York Times as a columnist and senior editor. This article takes a deep dive into how Target tracks customers, how habits are formed and how advertisers exploit them, and why pregnant women are such targets in advertising. It also looks into how Target avoids talking about its surveillance methodology (Duhigg was banned from Target offices). While Mindf\*ck helped me understand the psychology that goes into advertising, this explained how the science of habits plays into advertising. It also explains why pregnant women are such big targets, and how companies find them. Duhigg uses interviews, pre-existing psychology research, and his own expertise.

Feathers, Todd. "After Dobbs, Advocates Fear School Surveillance Tools Could Put Teens at Risk." *The Markup*, July 8, 2022. Accessed November 29, 2022. <https://themarkup.org/privacy/2022/07/08/after-dobbs-advocates-fear-school-surveillance-tools-could-put-teens-at-risk>.

This article was written by Todd Feathers, an experienced journalist covering surveillance and algorithms at the Markup, a newsroom investigating Big Tech. The article uses quotes from student surveillance software companies, school administrators, privacy advocates, and high school students. It explains the threat school surveillance poses to reproductive freedom, something I haven’t looked into before.

Gordon, Marcy “Democrats widen scrutiny of tech over abortion data privacy.” AP News, July 22, 2022, accessed November 16, 2022, https://apnews.com/article/abortion-technology-apple-inc-congress-government-and-politics-fa6dfd46baeb3732df4b4fcb720dd04a

This article was written by Marcy Gordon, an AP News journalist who covers tech policy. Using direct quotes from congress, personal expertise and current events, Gordon explains the pressure congress is putting on data brokers and school technology monitors. It was useful to my case because it explains the position congress is taking.

Hunter, Tatum. "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/.

Tatum Hunter is a technology reporter for the Washington Posts, a national newspaper. The article investigates the trackers on planned parenthood’s website using evidence from Privacy Lockdown, a cybersecurity company. The article explain a type of surveillance I hadn’t anticipated: non profit surveillance.

Hunter, Tatum. “Planned Parenthood Suspends Marketing Trackers on Abortion Search Pages.” The Washington Post. WP Company, June 30, 2022. https://www.washingtonpost.com/technology/2022/06/30/planned-parenthood-privacy-data/.

Another Article by Tatum Hunter about Planned Parenthood tracking. It uses quotes from planned parenthood announcing they would stop using marketing trackers as evidence. It helped update me on the state of security on planned parenthood’s website.

Keegan, Jon and Tarr, Donna. "Online Abortion Pill Provider Hey Jane Used Tracking Tools That Sent Visitor Data to Meta, Google, and Others." The Markup, July 1, 2022. Accessed December 5, 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.

This article is written by Jon Keegan and Donna Tarr, two reporters for the Markup, a newsroom investigating Big Tech. The article looks at trackers on Hey Jane’s (an abortion pill providers) site.It uses quotes from Hey Jane and privacy advocates along with evidence from The Markup into the trackers. It provided more information on non profit surveillance.

Meta, “Correcting the Record on Meta’s Involvement in Nebraska Case”, Meta, August 9, 2022, accessed November 16, 2022, <https://about.fb.com/news/2022/08/meta-response-nebraska-abortion-case/>

This is Meta’s response to the critism it got for handing over texts to Nebraska authorities in an abortion case. It’s a primary source representing the company's views, and it was useful to my paper because it provides a first-hand big tech perspective.

Fitzpatrick, Jen, “Protecting people’s privacy on health topics.” The Keyword, July 1, 2022, https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/

This is a source announcing new google privacy policy in July. It details their plans for location tracking (deleting location data in and near abortion clinics) and explains how it looks at government requests for data. It was written by Jen Fitzpatrick, a Senior Vice President at Google, and provides a first hand response of how Google addresses privacy concerns.

McCubbin, Sabrina. "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>.

This article was written by Sabrine McCubbin, A lawyer specializing in privacy. It summarizes the Carpenter v. United States case using the case as evidence with McCubbin’s expert analysis. It helped me understand the dissenting opinion, and third party doctrine.

“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>.

The National Conference of State Legislature is one of the top organizations that looks at policy and ideas across the country. This article looks at state legislation for digital privacy using law as evidence. It was helpful to my paper because it explained existing security laws in place.

Pew Research Center, “Mobile Fact Sheet,” *Pew Research Center*, April 7, 2021, <https://www.pewresearch.org/internet/fact-sheet/mobile/>.

Using data collected from surveys, Pew Research Center has statistics on how many Americans own smart devices, something helpful for me to understand how many people are experiencing surveillance. Pew Research center is a think tank about the trends of the world, run by social scientists.

Sisitzky, Michael and Schaefer, Ben, “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

This source explains the Public Oversight of Surveillance Technology (POST) Act, a key privacy law passed in New York City, it’s written by Michael Sistizky, the assistant director of the NYCLU and Ben Schaefer, in communications. The article is published by the NYCLU, the ACLU branch of New York, one of most established civil rights groups.

Su, Sara, “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/>

This article was written by Sara Su, a project manager director at Meta. It’s a primary source about Meta’s plans for encryption, which was useful for knowing their response to surveillance concerns.

Wiggers, Kyle, “Tech companies respond to US Supreme Court abortion decision” TechCrunch, June 24, 2022, https://techcrunch.com/2022/06/24/tech-companies-respond-to-u-s-supreme-court-abortion-decision/

This article was written by Kyle Wiggers, a technology journalist, about the response of tech companies to the Dobbs v. Jackson decision. It uses direct quotes from the companies to lay out their responses, all varying ways employees would be helped in accessing reproductive care. This was useful to my project because it shows the steps Big Tech was taking to protect its employees and gave their point of view.

Wylie, Christopher. *MINDF\*CK: Cambridge Analytica and the Plot to Break America*. S.l.: RANDOM HOUSE, 2019.

Christopher Wylie is a data scientist who worked at SCL, and then went on to help Steve Bannon form Cambridge Analytica. He was the Cambridge Analytica whistleblower. The book covers how Wylie came to work for Cambridge Analytica, the strategy Cambridge Analytica used, Overviews of social media behavioral manipulation in Africa, Myanmar, Britain and America. It ends with a proposed plan for legislators moving forward.This book really piqued my interest in my topic, and helped me understand the connection between tech/big data and politics. It gives a good overview of not only where and how our data is being collected, but also what is being done with it. It’s a good place to start. Wylie uses personal experiences from his work, personal expertise, and a review of research.

## 

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)