Taylor Cash Rose

Sharman Apt Russell

Project Period 1

Packet #2

Data Feminism

A few years from now, perhaps someone named Michelle opens her phone. Perhaps she lets out a deep exhale before typing in the search bar. She has to be careful about this. She knows to leave her phone behind if she physically goes even near a clinic to keep from being caught in increasing dragnet surveillance. Having the wrong app open in the background even now could mean an arm popping up like a stopped turnstile, barring her from entering the clinic. That arm might be attached to a police officer who would say something like, “excuse me, miss, can we chat with you for a second.” Then she would be sent off on a conveyor belt through the judicial system, shrink-wrapped in polyester, and stamped as a criminal. The prison system might return to its twentieth-century goal of “feminizing female prisoners.” Maybe the uniforms come with aprons.

Michelle would ask a few friends the best way to do this, what words to use or not, and what might flag her for tracking. They would tell her to stay away from the obvious ones: abortion, late period, mifeprex, mifepristone, anything that combined the words “women” and “clinic.” She deleted her period tracker app when she saw Gina Neff, professor of technology and society at the University of Oxford, tweet, "right now, and I mean this instant, delete every digital trace of any menstrual tracking.” This was the day after Roe was overturned. By 2026, it might still be common for people to get abortion pills or maybe even get face-to-face with a

doctor — but only if you know the right people or follow a digital trail without leaving a trace of your own. Regardless, a legal battle would throw people into a federal vs. state law hedge maze. No matter what, a subpoena for your phone would mow through it all. Now, several years after the overturning of Roe, if Michelle's phone or computer might be taken, she would go to jail just searching for options. Maybe her name is Michelle. Maybe it's something else. She is more than her name because she is a possible future.

***

By the afternoon of May 2, 2022, the Politico newsroom was ringing, the kind of breaking news tuning fork that sends reporter's fingers typing at twice the speed they normally do. They had a leaked copy of the US Supreme Court ruling that would eventually overturn Roe v. Wade, 53 days later. The leaked draft served an important purpose — it was a warning cry for clinicians to figure out what would become illegal and when. It was a signal for mutal aid groups to start sharing rideshare sign up sheets and gofundme campaigns. Herbalists propagated seeds for abortion gardens that might need planted in the years to come. Having a leaked ruling gave time for many activists to ready themselves.

After the leaked ruling, amongst the protests, and before the pledges from politicians and corporations, hundreds of articles appeared about the potential dangers of period tracking apps. The data inputs for a user vary widely, but most ask for things like the dates of menstrual cycles, medication, weight, mood, sexual partners, and location. Even running in the background, some of these apps collect things like constant location, purchases, search histories on browsers, and even photos. The fear is that the data collected in the apps could be used to see whether or not someone had an abortion, and that information could become evidence in a prosecution.

Considering that this has already happened, the fear isn't misplaced. In 2017, a Mississippi woman was charged with murder after having a miscarriage. The woman's search history (she had googled the word "abortion" late into her pregnancy) was used as evidence in the prosecutor's case. Two years later, the state of Missouri had the curtain ripped open, revealing their monitoring of pregnant people. The Department of Health director, Randall Williams, had inspectors reviewing Planned Parenthood's data to find people who had complications with their abortions. The data collected was used in an attempt to discredit Planned Parenthood, by compiling misleading information that women's health experts argue is within the expected range. (For clarification, maternal mortality rates in the United States is almost 3 times higher than any other industrialized nation, making abortion a safer option when simply considering medical facts.) The information Missouri officials gathered is technically outside the protection of medical privacy laws for the state health groups, meaning that there is debate about whether he did anything wrong. What is more concerning is that this practice is even occurring regardless of the reason.

This is not the first time that people with urteruses have been targeted by surveillance tactics. Reuters notes that "technology has long gathered — and at times revealed — sensitive pregnancy-related information about consumers." The article notes that in 2015 there were a slew of abortion opponents who were sponsoring targeted ads that would only show up for people coming in and out of reproductive health clinics. Using geolocation tags, the ads would appear and if clicked would push people to anti-choice websites. Digitally, these groups were able to stand outside of clinics across the country and bombard patients with anti-choice messaging.

At the time of writing this, 14 states have banned abortion with 8 others sitting in a legal limbo where the ban was opposed. When these kinds of surveillance campaigning tactics are used in states where abortion is illegal; data can become the ever-peering eyes of an authoritarian state. Bioethicist Arthur Caplan warned, "When a government official monitors your reproductive behavior, you are perilously close to replicating [a] totalitarian regime."

During a conversation for NPR's podcast Shortwave, health researcher Giulia De Togni shares about her experience as a user of the app Flo. She notes that any time her period is late she will start getting ads for pregnancy tests, trailed by ads for family planning services, and lastly baby items. This experience is not uncommon and it's actually quite lucrative for companies. NPR found that a pregnant person's data is worth 15 times as much as someone who is not pregnant. The thought is that those who are soon to give birth have a lot of upcoming expenses: Baby care items of course, new furniture, maybe a new car that is more reliable to get to and from doctor's appointments, perhaps life insurance or new budgeting apps. Big life changes are a meal ticket for hungry companies.

The data that can be gathered from a period tracking app is immensely valuable. Partially because pregnant people might be primed to spend more money, but broader is the goldmine of healthcare data as a whole. A study in 2019 found that 79% of health apps share user data. And considering that according to one study done by the Kaiser Family Foundation, nearly one-third of U.S. women have used a period tracking app — that is a vast amount of the population whose data is being bought and sold without their full, informed consent.

In Europe the flow of data is a drastically different terrain than the US. The GDPR — a set of rules that govern how some companies have to run their apps differently for European users — gives more transparency and control to consumers. This kind of limitation on digital

surveillance is similar to the Environmental Protection Agency's line in the sand for manufactures. When the EPA sets a limit on the amount of groundwater contamination that can come from a car factory in the United States, it protects the people who fish out of nearby rivers or spend summer afternoons tending to their garden. Both restrain companies from over-extraction.

Period tracking apps are an easy way to see the potential harm of data surveillance. Privately keeping track of one's health shouldn't be a way for a prosecutor to gather evidence. Unjust surveillance is a violation of privacy and crack in the foundation of a free society. Edward Snowden framed it well, "arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

Surveillance is the most concerning side effect of rapidly developing technologies, ranging from license plate readers to user-data gathered off of cell phones. These two examples are widely different in how they are used, but what they have in common is that government bodies have the ability to monitor daily activities. In the case of period tracking apps, they are a perfect synopsis of the dangerous potential of personal data being used as a means of surveillance.

For those who sit in traffic on I-285 and find themselves driving through the streets of Atlanta, it's not unlikely to have a photo snapped of their license plate number. That number, and where the photo was taken, will sit on a server — just in case Atlanta police need to know who was near a certain area on say, Tuesday at 3:57 p.m. Safety measures seem like a good reason to have this kind of technology. Afterall, having the ability to solve a crime quickly benefits everyone right? Atlanta is actually an interesting case study for this question.

Atlanta is, today, the most surveilled city in the United States. A program known as Operation Shield added surveillance cameras to light posts, buildings, underpasses, public and private places around the city. Atlanta Police Department reports that there are around 3,000 cameras, while other reports place it closer to 10,000 cameras. Most of these cameras are a CCTV, or closed circuit TV; think of the typical grey rectangular surveillance cameras that might be mounted on the corner of a business, facing the front door. In addition to CCTV-style cameras, Atlanta uses SiteView, cameras that can be easily installed on an LED street light. A private company called Flock Group Inc. makes the license plate cameras in Atlanta and many other cities.

There is a rather large chink in the armor of license plate readers — they are often not tethered to accurate information. Take The New York Times article that shared the experience of Brian Hofer in Oakland.

While Brian was driving down the highway in a rental car he suddenly heard sirens behind him, then more sirens. A swarm of police directed him off the highway and soon had him in handcuffs in the back of a cruiser, his brother kneeling outside with his hands up. The problem was that Brian's rental car was still reported stolen after many years of it being found. When a license plate reader caught the tag, it set off an alarm, calling police to the scene where the car was last seen. Considering that police killed over 600 people in traffic stops between 2017 and 2022, it is not unlikely that being pulled over for a license plate reader setting off a faulty alert would result in innocent people being killed.

Residents can sidestep some of this surveillance, or at least prevent the police or private companies from holding on to that data. Citizens can request that their data be wiped from police servers. Police will comply with these kinds of requests, within, well, limits. The Atlanta Police

Department makes sure to say that they will hold onto the information in the event of a crime, like a car being tied to an arrest warrant or a car theft for example. Unfortunately, it is no secret that this information is kept on the desks of police for far less altruistic purposes. The ACLU gathered 26,000 pages of documents, using Freedom of Information Act requests, that show "all of this data [from license plate trackers] is being fed into massive databases that contain the location information of many millions of innocent Americans stretching back for months or even years."

Law enforcement's ability to hold onto data is almost as concerning as the ways that they gather it. A practice called "dragnet surveillance" allows police to find the name of anyone who was near a certain area or who has searched for particular keywords. The Electronic Frontier Foundation warns about the dangers of dragnet surveillance — also known as "reverse demands," "geofence warrants," or "keyword warrants" — can show police if someone was near an abortion clinic or maybe a gender-affirming clinic. These warrants are not few and far between. Google alone received more than 5,700 geofence warrants between 2018 and 2020, all of which were from 10 states that have now passed anti-abortion and anti-LGBTQ legislation. These warrants are dangerous, showing the precise, long, winding fingers of an authoritarian reach.

***

Personal data seems to be a key link between over-policing and the foreshadowing of a world where pursuing bodily health is crime and conviction. What if apps, laptops, smart cars, simply couldn't collect information anymore? It might seem like the easiest solution — call it preventative healthcare for digital lives. However, a massive restructuring is unlikely. The growth of data brokers alone can attest to that — an industry that will reach $462.4 billion by

2031. Personal data will continue to be the blood flowing too and from big tech. Digital civil liberty activists do have solutions in mind and guidelines on where to go next. One of those paths could be data feminism.

Data feminism is an action and a position. It involves specific calls to action for big tech companies, but more than that, it is an ideology, a framework, the same as feminist theory. But before that, a way to understand data is through the lenses of property and labor.

If data were considered property, in the mind of legal scholar Salomé Viljoen, there would be two options. Salomé spends a lot of time thinking about the legal status of social data. Does it have protections the way that labor does? Is it actually more like property, one that can have legal regulations on how it's used and where it is sold? On the Tech Won't Save Us podcast, Salomé shares a futuristic view of what each of these paths might look like.

Take the option of labor rights. Data, after all, is the observation of something that is happening. Say, John runs every day. Every morning he wakes up, stretches, finds the right playlist, and hits "start" on an app called Map My Run. John's running creates data points that Map My Run tracks — where he runs, how often, what time of day, and where he is on his progress to increase his energy levels. The "work" that John does every day is of course running, but creation of those data points could also be considered labor.

Imagine that tomorrow social data is considered labor. Tomorrow morning, when John goes to lace up his shoes, he might see a monthly deposit notification for his bank. The amount would only be for a few cents, but in this tomorrow there are laws saying that he must be paid for every mile he toes into the pavement. If data were considered labor, John would also be able to join others who use the Map My Run app in petitioning Under Armour, the creator of the app — collective bargaining. Maybe they would ask for more money because health data is so valuable.

Maybe it would be illegal for Map My Run to have access to John's younger brother's photos, because he is under age — child labor laws. Viewing data as labor provides a framework for equity.

Now what if data was considered property? This framework gives new questions a seat at the table. At the head, who owns data? Is it the property of the people or big tech? Is it considered public property? If so, then shouldn't everyone have equal access to it? Are there rules about what that data can do? What about how it's maintained? If data were considered property, perhaps there would be regulations on the environmental impact storing data could have. Maybe there would be open access to certain types of data, giving small startups the same chances at research as huge companies. If data is a small sliver of property, then the people are entitled to compensation when it is taken from them.

Talking about data in the context of labor rights or property law gives many digital civil liberty advocates the language they need to write a more equitable future. These kinds of considerations are necessary parts of a democracy. Salomé even says that democracy is "a right of recognition in setting the rules that we are all mutually subject to." When the people are impacted by something, they have a say in where that impact can land.

So if labor rights and property rights can be frameworks for data management, what solutions reveal themselves when data is assessed with morality and equality as the crosshairs?

Data feminism uses feminist theory as a map while navigating the digital world. Ideals like consent become mandatory instead of an exception. Intersectionality becomes built into the research that assesses technology. Furthermore, queer theory helps solution seekers detach from binary systems and dream differently about how data could be used.

At the most basic level, feminism should be a given; “a feminist is anyone who recognizes the equality and full humanity of women and men,” as Gloria Steinem put it. Feminism in its most integrated form doesn’t stop at the doors of classrooms or in the ink of public policy. It is a way of seeing the world. A way to measure society. To see the impact that something has on all people. In the case of big tech, data, and surveillance capitalism, feminism is a way to talk about how these things impact people.

One of the core values of nearly every wave of feminism includes agency. First wave feminists fought for agency over their right to vote. Second wave feminists called for an end to sexist treatment and for personal agency at work and at home. Third wave feminism pushed personal agency forward through sexual reformation and brought the idea of consent into the zeitgeist.

Consent is a monumental part of feminist movements. It’s the personal autonomy to know what someone is signing up for. It’s the transparent “yes” and the respected “no.” Feminist scholars today would likely say that consent is a radical part of everyday life, not just sex. Consent is a recognition of power dynamics, seeing what’s at play in the room and who built the walls. When it comes to surveillance capitalism, the power dynamics are clearly in the hands of big tech. That power is like a ship line made of a thousand tiny threads. Data is only valuable when there is:

1. a lot of it

2. and a way to interpret it.

Big tech is able to gather massive amounts of personal data mostly by making it hard to avoid. The capital part of surveillance capitalism is financially worthwhile because data shows insights to what huge groups of people are doing and what they might do. It’s easiest for big tech

to gather this information without asking first — at least not *clearly* asking. Hiding the level of surveillance under molasses-thick terms and services makes it easy for people to check yes without knowing the full story. It's not likely that downloading a new app will soon come with a detailed breakdown of every way that gathered data might be used, who it could be sold to, and what it might help create. A lack of transparency is the bread and butter of big tech.

Data feminism is a futurist theory of digital democracy. A core attribute of data feminism is consent. Imagine a digital space where people knew exactly what information they were giving away, why it is valuable, and how it could be used? Imagine being told clearly that saying yes to an app having unlimited access to one's camera roll could be part of a sandbox that lets an AI train to further develop facial recognition technology. Imagine also knowing that facial recognition technology would be used by ICE to hunt down undocumented people and prosecute them. Would transparency change what people downloaded or checked "agree" to? Applying a feminist approach to data management would allow users to not only know these things ahead of time, but be informed of them as they change, and revoke their "yes" or their "agree" at any time. Digital democracy must have consent wired in, because consent is a foundational layer of feminism and therefore equality.

Feminism, thankfully, has grown out of the white, cisgender pot where it was planted. True feminism today is deeply intersectional and must assess equality through systems thinking — seeing the added complexities and nuances of things like race, gender expansiveness, and class. Race is an exceptionally important factor when discussing data regulation and reform.

Data surveillance is disproportionately exploiting and harming communities of color. Which sadly is not surprising considering the racist undercurrent in many modern pieces of technology. Take an automatic soap dispenser, for example. In order for near infrared technology

to register that there is an open palm, it must have light bounced back to it. This is a design flaw that was created without the consideration of skin with more melanin, which would absorb more light and therefore reflect less light back to the sensor. This kind of technology shows an important aspect that is seen elsewhere again and again — it was designed to function at its highest level only for white users. Facial recognition algorithms are known for frequently misidentifying people of color compared to the number of misidentified white people. Ruha Benjamin calls this racist theme "a New Jim Code," pointing to the eerie similarities between the systemic racism built into modern technologies and Jim Crow being built into American society. She gives the example of China's social credit system as a case study for the far reaching implications of inequitable design.

> Using proprietary algorithms, these apps track not only financial history, for instance, whether someone pays his bills on time or repays her loans, but also many other variables, such as one's educational, work, and criminal history. As they track all one's purchases, donation, and leisure activities, something like too much time spent playing video games marks the person as 'idle' (for which points may be docked), whereas an activity like buying diapers suggests one is 'responsible.' As one observer put it, 'the system not only investigates behavior, it shapes it. It nudges citizens away from purchases and behaviors the government does not like.' Most alarmingly (as this relates to the New Jim Code), residents of China's Xinjiang, a predominantly Muslim province, are already being forced to download an app that aims to track 'terrorist and illegal content.'

This type of tracking, that uses already prejudicial bias as an implicit truth, is how technology will evolve in a way that injures democracy and inflames oppression. Ruha gives the example of hostile architecture in a public park — the benches built with armrests in the middle to make the space uncomfortable to lay down in the hopes of preventing unhoused folks from lingering — is not unlike what is happening with the design of many algorithms and data

practices today. The same way that discriminatory design practices are embedded in hostile architecture, it is also embedded in the digital world.

Audre Lorde's famous quote "the master's tools will never dismantle the master's house" rings astoundingly just as true for technology as it does for society injustices. Even the most generous assumption — that racial and other injustices are not being purposely bred into technology — still sheds light on a problem. That technology is being taught to behave like humans, including biases.

Take the example that Ruha notes, where in 2016 it was pointed out that if someone Googled "three Black teenagers" mugshots would immediately come up. Whereas if someone Googled "three white teenagers" smiling faces would appear. The shrugged off answer from Google was that the search engine tries to predict what someone wants when they are searching. However this is still a perpetuation of a deeply racist ideology, and it brings forward an important question: if an algorithm is supposed to make a more advanced decision than a human can make, then what does that advancement look like when it is a bolstered version of oppressive systems before it?

Questions like this are not new. In fact, scholar Catherine D'Ignazio, assistant professor in the Department of Urban Studies and Planning at MIT, co-wrote a book called *Data Feminism* that raises these same types of concerns. (Her book focuses on a more expansive definition of data, including all research data, which is beyond personal surveillance data that is being discussed here.) An article from the University of Pittsburgh notes:

> D'Ignazio said they wrote the book because they saw data feminism as part of a growing body of work that aims to hold elected officials and corporations accountable for making racist, sexist and classist data products. Examples include face detection systems that can't recognize women of color, hiring algorithms that downplay women's resumes and child abuse algorithms that

> punish poor parents, she said. D'Ignazio said that this growing body of work has created an 'exciting moment to be thinking about issues of power and justice and data.'

Her work around data feminism expands on important questions for technology and in how large sets of data are analyzed. In a recent interview, she gives the example of how data is assessed regarding the homicide rate in Mexico. It is frequently recognized that many women are systematically murdered throughout the country, however, very little data exists to bring attention to the issue. The problem, in this case she is talking about research data, is how the information is being interpreted. Bringing a feminist approach to data evaluation and interpretation is valuable in the way personal data is gathered off of phones and other pieces of technology.

Data feminism addresses the systemic racial, gendered, and class oppression that is perpetuated by technology. Establishing a critical feminist lens of data is vital. Data is power in an increasingly digital world, and feminism, at its core, is deconstructing power dynamics to create a more equitable society.

Where potential really arises is applying queer theory in the same way as feminist theory — as frameworks for assessing how data is gathered and why. Queer theory demands transformation and constant adjustment. "'Queer' not as being about who you're having sex with (that can be a dimension of it); but 'queer' as being about the self that is at odds with everything around it and that has to invent and create and find a place to speak and to thrive and to live," as bell hooks said.

As feminism has evolved, snowballing to include radical action that addresses the holistic lives of people, it is now innately connected to the ideals that have become queer theory. An important part of queer theory holds evolution at the epicenter. The word "queer" is a verb that

encompasses constant change and exploration. “To queer” is to question existing structures and binaries, are they really “normal”? By nature, the concept of queerness often involves discovery and a shift in how one sees the world. When digital society is assessed through a queer lens, it brings up questions like, what if we collectively questioned how data was extracted from us? What would it look like to create a new “normal” where we could use the power of that data *for* the people instead of the profit of big tech? As a collective, when we divest from corporate power we are inherently “queering” the way we think about digital democracy.

There are many viewpoints that become clear when using queer theory as a lens to assess the digital world. As Kevin Guyan wrote in *Queer Data: Using Gender, Sex and Sexuality Data for Action*, “heightened data competence can therefore ensure data is used to improve the lives and experiences of LGBTQ people rather than only serve the interests of, what Catherine D’Ignazio and Lauren F. Klein described as, the three S's: science (universities), surveillance (governments), and selling (corporations).” There is immense power in data collection. If personal data was treated as, say, a universal right — to revoke it, to see how it is used, to access it for research, to use it for the collective good — the wealth that comes with data would be shared.

Using data in ways that divest from corporate power and control is not unheard of. The former leader of the Social Democratic party in Germany, Andrea Maria Nahles, suggests that data can be a public good. Say after 10 years data sets about consumers became a public resource. Imagine somewhere like a library housing this data and making it available for researchers to access who are using it for the public good.

A very realistic example of an alternative pathway is the city of Barcelona. Barcelona has a municipal approach to citizen data, where it is managed for the public good. So tech companies

who come to Barcelona have to turn over information to the city, the city manages that data as a resource for the public good. When information about the public is used this way, it becomes a sustainable resource.

Using queer theory as the design template for digital democracy creates endless potential and fosters sustainable decisions. Instead of building facial recognition software that is used to police communities of color, that effort could be spent tracking water usage, creating more sustainable cities that can endure the disruptions of climate change and use resources in an equitable way. Instead of developing algorithms that reinforce cycles of poverty by denying loan applications, that same effort could be spent tracking wage violations, processing data about the number of women who are killed each year, or helping provide access to the thousands of transgender youth who need shelter and healthcare. These ideas are not impossible, but they do require collective dreaming.

***

Down an alternate timeline, perhaps Michelle sits on a park bench waiting for the bus. She is on her way to an appointment at a clinic. The online check-in system sends her an alert that the doctor is running a little late today. A bus pulls up. Hers is the next one. Since the city started tracking public transit instead of electric cars, more money was routed to improve the fleet — longer hours, more route stops, and an app that shows where the bus is in real time. The improvements allowed her to sell her car.

She looks across the street to where a greystone building has the black smudged silhouette where the letters IMPD once were emblazoned above the door. Over the last few legislative cycles the line items for police budgets seemed to be shy a few commas from years before. The research feeding into crime states dried up when camera and license plate

surveillance companies couldn't sell the data they gathered. She could hear the hum of a bumble bee behind her. Last year the city discovered the massive amount of water waste that was caused by keeping the park grass limited to blue grass. Now, there were tufts of native meadow grasses — a more hospitable home for bugs and required far less water. A notification popped up on her phone, the bus was around the corner.