Book Proposal

# Empire of Insight

How surveillance tech is killing the planet and arming a police state

by:

Taylor Rose

by:

Taylor Rose

(317) 220-5380

taylorrosewrites317@gmail.com

# Overview

When we hear “green tech” most of us don’t think about the Chicago police officer sitting behind a desk watching a transgender activist move around the city. We probably don’t think about an apple farmer in Oregon who can’t access the software that powers their tractor every morning. The undocumented immigrant who is picked up by ICE, just because he walks past a neighbor’s smart doorbell on the way to work, is likely not the first person who comes to mind when we talk about climate change.

But all of them should be.

These seemingly separate stories are all real examples of “green tech” in action.

Tech is often presented as the magic wand that can make climate change disappear, just a half a degree before it's too late. There are some aspects that are promising. Carbon removal from the air does work, but it’s incredibly expensive. There is green tech that can pull saline from the sea to offer clean drinking water. There are roads that can absorb flooding and can charge an electric car while it drives. There is even a tractor that might soon run off of methane while it rolls through a field.

However, the green tech that we are far more likely to encounter on a daily basis is all around us. It’s presented as the “small choices” that we can make to help the planet and soothe our collective climate anxiety; it’s the electric car charging stations; it’s the smart thermostat that sets itself; it’s the AI-powered traffic camera that a local official just approved.

They are all pieces of what this author calls “technotranquilty” — how big tech companies are using climate change as an excuse for unlimited surveillance, and police are the

best customers.

There are many pieces of "green tech" that are valuable, only because it watches you.

***

*Empire of Insight* is a collection of reported essays and speculative nonfiction. It uses thorough research and asks "what if" to paint a picture of our urban horizon. This work of speculation — both of a positive potential future and a warning against a dystopic path if we do not change — shows how the same tech we hope will save us from climate change is pushing us to consume more and is now the tactical tool of a growing police state.

Consider this the revolutionary's guide to data surveillance, abolition and anti-racist tech practices, and a conversation starter on how we can create positive alternative futures.

## CHAPTER 3: The Panopticon of Police

A November sun was shining, thin and nearly worn through by winter around the corner. It was only mid morning and several hundred people had already gathered in front at the tri-layered fountain in Millennium Park. Bronze seahorses dipped, dove, and rose out of the water. Mouths cast forever open seemed to echo the crowd:

"From the river to the sea, Palestine will be free."

The crowd started first as a trickle, then as a steady stream from LaSalle, and before that, the headwaters of buses and train platforms. Soon, several thousand protestors wrapped in keffiyehs arrived, holding painted cardboard signs, black, green, and red.

The protest slowly spilled over and started flowing into the road. Soon it filled all eight lanes of Lake Shore Drive, causing traffic to come to a parked gridlock. News helicopters vibrated and pulsed like hummingbirds overhead.

The protesters marched along the park and through the road, eventually reaching a dam of police barricades, metal fence pieces to keep them from going north or south. Every few minutes, the police seemed to divide and multiply like cells; where there were two, there were four, and where there were four, there were suddenly eight. Tensions bloomed and billowed like smoke from a leafy fire. The police waved batons like incense.

The police and protestors pressed closer and closer together. The metal barricades levitated off the ground — both sides hoisting them in the air to use as plows and shields, pushing forward in one motion and being pulled back into the tide by the other's movement.

A few protestors scaled traffic lights, hanging off of crosswalk signs with one arm, using the other to take videos with their phones or to lead chants against the police. From this perch, they were eye level with metal boxes mounted to light poles across the street. If these protestors looked closely they would see a twisted vine of wires on a light pole across the street, snaking upward to what looked like two massive bug antennas stretching out over the crowd.

This seemingly unremarkable species of urban infrastructure hanging over the protest have themselves caused many protests. This particular hunk of metal and wires is actually a

high-tech microphone called ShotSpotter. It's a small piece of "smart city" tech that is intended to identify the sound of gunshots. One of the problems is that while it does identify some gunshots, it also is well-documented in causing others.

On March 29, 2021, a ShotSpotter microphone pinged an alert to Chicago police, telling them that there was gunfire in Little Village. When officers arrived in the mostly Hispanic neighborhood, they saw two kids. One was Ruben Roman, 21 at the time and quickly ran from the police officers. The second, was a child named Adam Toledo, who was 13 years old. Body camera footage from officer Eric Stillman shows Adam running down an alley. In it, Adam stops, panics, and tosses a gun over a fence. He then turns to face the officer, surrendering, with his hands raised. He is shot through the chest a moment later.

The murder caused massive protests in Chicago. Many activists noted the fallibility of the ShotSpotter technology that brought the police to Little Village in the first place. And as the case moved its way through the court, and when Eric Stillman was charged and arrested, part of the evidence that was called into question was the notification from ShotSpotter — although the boys had a gun, it's very likely that there never was a shot fired. It's likely that the notification was just one of many in a fallible symphony of false positives. A study by the company itself found that everything from church bells to trash trucks are mis-identified as gunshots. It's likely that the police arrived with a version of the truth already playing out in their minds, and chose to live within it instead of responding to what was in front of them.

ShotSpotter has since made headlines around the country. In Chicago, there are over 2,500 of these microphones throughout the city. The vast majority are placed predominantly in

BIPOC neighborhoods. When “smart city” tech like ShotSpotter is placed in a neighborhood that the police assume has more violence, and those police start to show up to disproportionately more calls from that area compared to others, it quickly labels the footsteps of a city and the common-place sounds of urban life as indisputable proof of violence. The result is a self-confirming loop, playing on repeat.

An investigation from AP found a report from the Office of Inspector General’s Public Safety sector, stating that the data “does not support a conclusion that ShotSpotter is an effective tool in developing evidence of gun-related crime.” The Inspector General’s report also showed that between January 2020 and May 2021 — in just a year and some change — ShotSpotter altered police to 50,000 gunshots in Chicago. In reality, there was only a gun-related crime with around 9 percent of those instances. Extend that time frame to over five years, like a study by the Cook County state attorney’s office did, and we find that less than in less than 2 percent of the 160,400 ShotSpotter alerts led to arrests. The tech’s AI system often misidentifies live gunshots for what is actually fireworks or a car backfiring or other noises that happen fairly often in a large city. ShotSpotter does have employees who prepare forensic reports for criminal investigations. These reports often have similar mistakes, claiming that a certain shot was toward a police officer when other evidence shows that either isn’t true or can’t be known.

What happened to Adam was horrific and sadly not a lone exception.

Take Michael Williams, who, sat in a jail cell contemplating suicide nearly a year after he was arrested for a murder he didn’t commit.

Rewinding back to the night he was arrested, Michael was lying in bed with his wife, not able to sleep. He went out to buy a pack of cigarettes from a nearby gas station. He pulled up in his car and saw that the gas station had the windows broken and appeared to be robbed. Looting was on the rise in the city of Chicago, since just a few days before George Flyod was murdered by the police.

Michael, a 65-year-old Black man, turned his car around and started to drive away. Not far away, a young man that he knew from the neighborhood waved him down and asked him for a ride. Michael, of course, said yes since he knew the man. The two stopped at a traffic light, and another car pulled up next to them, pulled out a gun, and fired into Michael's car. The bullet hit the young man in the passenger's seat. Michael rushed him to a hospital, where he unfortunately died a few days later.

After three months, the Chicago police come knocking on Michael's door, saying they have a warrant for his arrest. He was charged with first-degree murder. The evidence was a ShotSpotter audio triangulation that the police said proved that Michael pulled the trigger inside the car. The prosecutor also used footage from a traffic camera — where the car that actually fired the shot appeared to have its windows up — as further "evidence" against Michael.

Michael had no offenses in the last 15 years, but before that had a criminal record. The faint trail of crime, combined with two pieces of data that proved to both be inaccurate, led to Micheal being arrested and waiting for a court date. For nearly a year, Michael sat in a prison cell. He looked forward to the phone calls with his wife where she would remind him of fishing trips with the grandkids, as the AP story shared. After nearly being lost to the prison system and frozen there by a crime he didn't commit, Michael was finally released.

While Michael's story garnered national news for a while, the pool of media attention shrank and drained away, leaving only activists and Chicago residents still talking about the impact of the tech. One of the activist groups, The MacArthur Justice Center, filed a class action lawsuit against the city on behalf of Michael and 82 other Chicago residents who were the victims of CPD using physical force against them during a ShotSpotter deployment. One of the plaintiffs was Dennis Ortiz, who was at a laundromat washing his kid's clothes when the police pulled up and arrested him. Another plaintiff, Derek Scruggs, was arrested in the parking lot of his work. The suit notes that he was detained and forced to submit to a humiliating body search before being released after the police realized that the ShotSpotter system provided them with bad information.

Activists continue to campaign against gunshot surveillance tools like ShotSpotter. During the election of Mayor Brandon Johnson of Chicago, organizers demanded to know how the candidates would respond to the end of ShotSpotter's contract that was set to expire in 2023. One of soon-to-be-mayor Johnson's talking points on the campaign trail was a promise to not renew the $8 million a year contract, not knowing that Mayor Lori Lightfoot had quietly extended the contract well before the three year contract was up.

Black and brown men, specifically, are paying the price for ShotSpotter's extended stay in Chicago. The MacArthur Justice Center, reported that the microphones are scattered over the 12 police districts with the highest percentage of Black and Latine residents. Roughly 80% of Black Chicago residents and 65% of Latine Chicago residents live in earshot of a ShotSpotter microphone. That percentage is nowhere near the same range as the percentage of white Chicago residents, only 30% live in the radius of ShotSpotter.

This kind of disproportionate placement of surveillance tech — where more devices are set up in BIPOC neighborhoods — is what kickstarts a long chain of events that become a continuously turning wheel, forever moving with its own momentum.

Chicago is one of the many urban areas that is considered to be both a smart city and heavily surveilled. Chicago has 32,000 cameras and has the second-largest local police force in the country, just behind the NYPD.

Now, picture a researcher who works in this city. They are tasked with tracking crime data that comes from those thousands of cameras and other smart city tech to see if the police surveillance tools are accomplishing what it's supposed to.

Say a neighborhood on the west side of the city seems to be a hotspot for robberies and shootings. The researcher finds that within a few blocks, there are several pieces of tech that are feeding them this information. So they start by mapping out where the tech is located; all the different forms of surveillance the police have started using like gunshot detection microphones, traffic light cameras, pedestrian surveillance cameras that are fed into a facial recognition system, and the footage of nearby businesses and homes with Ring or CCTV cameras. All of these tools seem to be showing that there is a steady rise in crime in this neighborhood. So, the researcher starts tracing the data to see whether this is true.

They find that these pieces of tech are fairly new, most of it being installed in the last few years. The increase, you find out, was because the police were asked where they suspected a large number of crimes were committed. Where could having this kind of tech present and gathering information 24/7 be helpful?

Once the tech was installed, it started lighting up. Gunshot here. A suspect lives there. Peering through the police logs shows that more officers made that neighborhood part of their daily patrol. Police started to stop more residents in this neighborhood. Maybe the officers stood shoulder to shoulder at a police station water cooler, talking about how the tech-led them to more arrests in the neighborhood. Maybe they nodded and no one seemed too surprised. More police officers started to show up and more arrests were made.

The researcher compares this neighborhood with others around the city and finds that after a few years of arrests, that area now has maybe double the amount of surveillance tools. It seems on a surface level that the new tech is doing exactly what the police want it to — acting as an eternally awake officer that is forever frozen at its post. The tech is simply documenting what already exists there, right?

The researcher leans back from their desk and wonders. Is crime really going up in this neighborhood or is it going up the more that it is surveyed? Would this be happening if the tech wasn't there? Can watching something cause it to happen?

The cycle that they just observed is a perfect cocktail of frequency illusion, confirmation bias, and systemic racism. On a much larger scale, the stats on race and crime have a long history of following this same recipe — where the stat becomes the reason that someone is discriminated against, then causing the stat to rise.

The assumption confirms itself into reality.

Take the example of a neighborhood that is subjected to systemic racism and over-policing. Those neighborhoods were often at one point watched closely by police, leading

to more arrests in those neighborhoods (after all, it's hard to make an arrest where there isn't a police officer).

More arrests become the reason why more surveillance tech is placed in those neighborhoods, which leads police to make more stops — and the NCAA noted that police are five times more likely to stop a Black person compared to a white person — and therefore more arrests, all of which might be based on faulty information.

Receiving "accurate" or "inaccurate" information often isn't what matters when it comes to surveillance tech. What does matter is if the information that police are receiving confirms or contradicts something they already believe. A study from the Dutch National Science Foundation found that police officers will follow the recommendations of an AI if it confirms something that they already thought. Subconsciously they start taking certain alerts, or alerts from certain areas, more seriously. This confirmation bias becomes an added layer of an ouroboros loop, that instead of shrinking, gets stronger with every bite.

***

The tech that police often use to conduct ongoing surveillance is a long list: it means automated license plate readers, cell-tower simulators, drones, video surveillance, traffic cameras, and smart doorbells like Ring.

Of course all of these pieces of tech aren't inherently bad.

Like smart city data, the information gathered can be used to create a safer and more sustainable city. A traffic light or speed camera can help cut down on pedestrian deaths. An

automatic license plate reader can help stop a kidnapping in progress. A gunshot detector can identify the sound of a pistol being fired and get an ambulance there faster to save a victim's life. But what happens when that information is wrong? What happens when that information is not only wrong, but the first response is to send in police who are trained to arrest or escalate based on bad information instead of assisting? These kinds of questions aren't speculative. And they point out what is at risk with ever increasing surveillance.

There is a distinct overlap between the tech that police can use for surveillance and the tech that is built into smart cities. There is an even stronger connection between the two when we consider the future where police might have access to every piece of smart technology as a way to continuously monitor and watch citizens. There is a possibility of this tech being used entirely as a means of police surveillance. In fact, smart cities are far too often a way of greenwashing what could easily become the eyes of the police state.

And in some ways, this is already happening. There is overlap in how data is managed, but in a far more direct way, the tech can look incredibly similar.

Take a traffic camera.

Mostly when we don't think about traffic cameras until we see the ticket in the mail after running a red light, but in addition to nabbing red light runners, the camera is constantly checking the license plates of every car that stops at that light too. Police tend to justify license plate readers by saying that they are checking to see if a car comes up as stolen. A smart city planner would say that license plate readers can more accurately monitor the flow of traffic and commute patterns, which could be used to redesign city streets or adjust public transit

times. A driver in Atlanta, like Brian Hofer, would say that license plate readers led to being in handcuffs for a crime he didn't commit. The New York Times shared the experience of Brian.

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 the 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 could result in innocent people being killed.

Today, Atlanta is 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.

Most of these cameras are CCTV, or closed circuit TV; think of the typical gray 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 LED street lights. A private company called Flock Group Inc. makes 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 untethered from accurate information and are disproportionately used as evidence against Black and Brown citizens.

Sadly, the story is not that different back in Chicago, either. The license plate reader system in Chicago includes everything from parking, red-light, and speed monitoring cameras — all of which fall under the same umbrella. ProPublica found that Chicago's license plate readers and ticketing systems have disproportionately been used against Black and Brown drivers. Zip codes with mostly Black and Latine residents received twice the rate of tickets as those in predominantly white zip codes. The tickets, court dates, late fees, and other added costs have sent tens of thousands into bankruptcy.

Citizens can partially conceal themselves from the line of sight of these types of traffic cameras and slow down the flow of their data when it comes to police 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 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."

But there are those who are dreaming and designing ways to sidestep that reach; particularly when it comes to facial recognition systems — like a clothing designer in Milan.

A video demo for designer Rachelle Didero's new clothing line cues up.

There is a dull whitewashed glow of a fluorescent light filling a screen. The angle looks like a security camera pointed at maybe a lobby, maybe a subway station. One by one, people appear in front of the camera and look up directly into it. Within a second or two, a square flickers around the person's face as the camera triggers an AI algorithm; it thumbs through thousands of pieces of data to pair them with their name.

Martha Hall. Brook Anderson. Ying Lee. Giraffe.

Yes, giraffe.

The fourth person to walk up to the camera has on a knit crewneck sweater, patterned with what looks like a neon-colored giraffe print, spun and twisted as if through a kaleidoscope. The pattern is an intentional design that is meant to confuse facial recognition software. It, along with other pieces like it, are a part of The Manifesto Collection from Cap_able, the clothing company that started as Didero's PhD. She has since won a prestigious intentional design award for the initial designs demonstrated in the giraffe video. The line of clothing all has similar patterns and designs; and is a small example of resistance against surveillance technology.

Activists around the world are familiar with protest safety tactics — things like concealing tattoos, covering the brow line, or wearing a mask over the mouth and jaw are ways

to prevent identification software from finding a match for protestors, potentially prosecuting them. Certain patterns, like the ones in Didero's collection, can also cause facial identification tools to fail.

Considering the inevitability that facial recognition software will continue to become more accurate with the backing of AI, it's become vital to understand how and where it's used. In the US alone there is widespread use of facial recognition among police departments, ICE, and federal agencies. Politico reported that New York, Chicago, and Los Angeles' police departments all use facial recognition. The true number of law enforcement groups that are using facial recognition is hard to know. One report said that the Government Accountability Office survey in 2021 found that 20 out of 42 federal law enforcement agencies use facial recognition.

Back at the protest in Chicago, on the same light pole as the bug antenna microphones, there is a "smart city" camera is as much a connection between Palestine and Chicago as the protest itself.

Chicago police run the feed through facial recognition software called Clearview AI — a leviathan of a tool that draws its power from our social media posts, holding the equivalent of 14 photos of every person on earth. The ACLU stated that "*neither the U.S. government nor any American company has ever* compiled such a massive trove of biometrics."

Its competitor, Oosto, is at that same moment being used by the Israeli military 6,169 miles away and is now programmed into drones. Oosto helped to create the draconian Red Wolf

tech in checkpoints in the Gaza strip. The tech is used by soldiers to monitor, control, and track Palestinians. It acts like a digital razor wire.

The tech, although now limited to private companies, still has an extensive reach. Law enforcement can use the tool readily, and before the ruling in Illinois, anyone could easily say they were a police officer and access the tech without further verification. Clearview AI has reportedly been used in the war in Ukraine to identify Russian soldiers and spies. There is unconfirmed speculation about Clearview AI being adapted to military drone technology; which is not unfounded, considering that a similar tool called Oosto sold a patient to put its facial recognition tech into drones, according to Forbes.

Oosto's facial recognition is used across the globe today in dozens of industries; it's used in casinos to try and catch people counting cards, sports stadiums to verify tickets and as added security, and by private companies as surveillance cameras with brains. However, Oosto is most known for being a go-to weapon of the Israeli military.

Oosto — an Israeli tech company — helped to create the draconian Red Wolf tech that is used at checkpoints in the Gaza strip. The tech is used by soldiers to monitor, control, and track Palestinians living in the Gaza Strip and acts like a digital razor wire gate that opens for some and closes for others.

A report from Amnesty International calls Israel's Wolf tech an "automated apartheid" which is not far off. Wired even referred to the West Bank as Israel's surveillance laboratory. The "wolf" tech consists of Red Wolf and Blue Wolf. The two are different aspects of the facial recognition system. Blue Wolf is an app that Israeli soldiers use. They are instructed to take as many photos of Palestinians as possible and upload them to the Wolf database. Wired quoted an

NGO made up of former Israeli soldiers called Breaking the Silence that said “prizes were offered to different units based on how many Palestinians they could photograph within a week.” Red Wolf is the facial recognition system itself and the algorithm that identifies people walking past Israeli CCTV cameras.

What the system looks like in practice, is something like this.

A Palestinian is walking to work. To do so part of his route takes him through Checkpoint 56 in Hebron. As he approaches, he sees up ahead a gate blocking a narrow roadway between two buildings, pale brick framing the blue sky overhead. As he gets closer he sees just how tall the metal fence really is; the top nearly touches the third-story windows in the buildings on either side. Two metal turnstiles serve as the doorways to enter and exit through the gate. Once he walks through one it leads to a small enclosed area before exiting through another turnstile on the other side of the gate. Perched at every angle are 24 cameras that started scanning his face while he was 100 meters away. The cameras snap photos of him and start running it through the Wolf database. Because he has to walk through Checkpoint 56 every day, the system quickly matches him to photos. The system sends an alert to one of the Israeli soldiers who stands in his path on the other side of the gate, saying that he can continue. The other alerts read things like “arrest” and “question.” In this moment, the soldiers know everything about this man. They know his name. They know every member of his family. They know where he lives and when he was last there. They know every interaction he has had anywhere near one of the Red Wolf cameras.

While this Palestinian man can cross through the checkpoint without being detained or questioned, that is not the case for many. Things as small as being arrested once at the age of 16

for having a knife can cause someone to be flagged as “arrest” any time they are near one of the Red Wolf cameras.

What we do know about Red Wolf is limited, mainly because the most in-depth report out there was conducted by Amnesty International who were limited to researching Hebron and Israel. They were not able to conduct any research in the occupied West Bank or the Gaza Strip — areas The Human Rights Watch called the world’s largest ‘an open-air prison’ —where the surveillance is (was) likely much worse.

The police are just one small aspect of the US connection to Israeli tech — a relationship that is well documented and the subject of many books. The AI needed to power the facial recognition software that monitors Palestineans requires a lot of computing power and data storage. Microsoft created cloud storage for Israel that is specifically for “public safety and justice” and data from IoT sensors. This type of cloud server support in Israel has been well-documented from other tech companies too. Both Google and Amazon entered into a $1.2 billion contract called Project Nimbus, that provides the data infrastructure for the Israeli military and government. A letter from Google and Amazon employees, begging their employers to break the contract, states, “This technology allows for further surveillance of and unlawful data collection on Palestinians, and facilitates the expansion of Israel’s illegal settlements on Palestinian land.”

The letter was met with no change from both tech companies. The amount of profit that comes from the relationship between Silicon Valley and Israel is far too valuable for both sides. Just one example looks something like this — Israel creates the tech, and Silicon Valley gets paid to process the data from that tech. The more that is surveilled, the more computing power is

needed. The two systems feed one another in a perfect capitalistic dream that never stops growing.

This same self-reinforcing relationship model has been proven to work through a case study that ironically is exactly where this chapter started — with the police.

Predictive policing in the US could be, at the moment, the poster child for what is wrong with unchecked data surveillance. The concept itself sounds like a dystopian sci-fi prompt, which was when "The Minority Report" was first written as a novela in 1956 by Philip K. Dick. The concept of making someone guilty before a crime is committed seems more far fetched than it actually is. To the police, it is not far-fetched at all. In fact, it started to make law enforcement really salivate around the financial crash of 2008 — a promise to be able to police more with fewer salaries to pay.

The idea of predictive policing started to snowball in the US much earlier though. (A well-researched paper called "Predictive policing management: a brief history of patrol automation" by Dean Wilson at the University of Sussex* shares a historical timeline that layers police ideology with technological change, as noted below.)

Predictive policing can technically be traced back to the 1920s when August Vollmer put the Berkeley police force in cars and on motorbikes. With this came a sweeping wave of technology in policing. Crime labs and handheld radios led to what would become federally-funded research that was outsourced to private institutions. In 1967 it was "The Task Force Report" created by the Institute of Defence Analysis, a group that researched military missiles and nuclear war. The report took the momentum that police forces around the country

were gathering and provided it with an analysis of tech — and more specifically, the mathematics behind "systems analysis." The result was a report that speculated a future state of policing that used computers as a way to automate police decisions, actions, and placement. Computers were just starting to be used by police when IBM created a model for the Saint Louis Police Department a few years earlier. Applying system analysis to policing led to a gold rush over the coming decades of police departments trying to gather and track as much data as possible.

As the financial crisis in the 1970s bloomed in the wake of the oil crisis, police were scrambling to justify their budgets. Data became an important current that police forces needed to keep running. Law professor Herman Goldstein was the one who saw the frantic struggle that police departments had as they tried to justify their expense. Goldstein noted that police had reached their peak; 'the situation is rather like that of a private industry that studies the speed of its assembly line, the productivity of its employees, and the nature of its public relations program, but does not examine the quality of its product.' Goldstein asserted that police were instead meant to be problem solvers and actively find solutions to societal problems. This concept became known as "problem-oriented policing." Under this creed, police were justified as the designers of public safety products.

Another justification for police came from COMPSTAT in the 90s, a database that stood for computer statistics. One of the cash crops that produced a ton of data for COMSTAT was the policing theory that a famous *Atlantic* article referred to as "broken windows."

"Broken windows" was the idea that if police came down harder on smaller crimes, like breaking a window, it would lead to a reduction in crime overall. It became a widespread

ideology in police departments. “Broken windows” was carried forward by a bannerman who had one of the most influential roles in US policing systems today, William Bratton.

He is most well known for leading three of the largest police departments in the country, Boston PD, Los Angeles PD, and New York PD. (With a militant approach to policing, he was brought out to Los Angeles immediately after the Rodney King riots.) Bratton was an evangelist for “broken windows” policing which generated a large amount of police-related data and was stored in a COMPSTAT system. He was also known for seeing the early capabilities in police data collection, predictive policing, and data automation to synthesize and understand that information instantly. Wilson quotes him directly, saying, “By streamlining data entry and automating it, and then developing a more robust capability to data mine, we will move closer and closer to real-time.” COMSTAT eventually fed into predictive policing tools like PredPolTM, a standalone predictive policing software that is widely used today. While Bratton was developing COMSTAT he worked shoulder to shoulder with one of the largest corporate funders of the police, Target. The chain retail store, Target, has partnered with police departments since the mid 90s. The company has one of the most well-known and sophisticated ad targeting algorithms in the marketing industry — using purchasing patterns and data that the company buys to build detailed profiles of every customer. Target has been a prime customer for period tracking apps, for example. Knowing when a customer is pregnant to send them ads for baby clothes is too valuable to pass up. The company also has some of the most elite employee tracking capabilities, monitoring the speed and productivity of Target employees with predatory precision. Target also has large forensics labs that allow their tech to essentially be rented. The company often funds CCTV installations in neighborhoods around their stores and supplies police with geo-tracking software to keep (often) Black and Brown citizens away from the area.

*Slate* reported that "since launching, SafeZone has become a 501(c)(3) nonprofit, independent from Target. It's also expanded to include other initiatives over the years like interactive crime mapping, text tipping, and a program in which members go to court proceedings to tell the judge how seriously the community is worried about crime." Bratton, like many other police chiefs, worked hand-in-hand with the un-ironically named corporation.

Bratton's work with Target is a perfect mirror for us, showing how the interests of big corporations and a police state are the same — to watch, to control, to siphon as much money from us as possible, whether that be from tickets, the prison industrial system, or targeted ads based on our buying habits.

Predictive policing has become a golden goose, one that consists of police departments being a constant producer of policing data and an eager purchaser of access to its insights. Realistically, police have no more incentive to disrupt this cycle any more than Silicon Valley does to speak out when its tools help execute a genocide. Data surveillance makes police departments too much money, and it's fueled by as many "broken windows" as they can find. Predictive policing is now a cottage industry the size of skyscrapers.

***

Surveillance tech has long been compared to another physical architecture of imprisonment — the panopticon.

The panopticon is a type of prison construction from the 18th century. The massive cylinder building was designed so those who were incarcerated were watched, without knowing it, at all times by a single guard. Today, panopticons are rarely used. Within them, sound reverberates and echoes to a near deafening level, and is considered cruel by even

American prison standards. Being forced to live in one robs inhabitants of their humanity.

But we do not have to live this way.

What if we had “the people’s right to data,” granting sovereignty away from the tech empire?

What if we took the microphones used to listen for gunshots, and turned it to listen for birds and bugs — telling us if an ecosystem is regenerating?

What if, instead of disproportionately giving tickets to drivers in lower income neighborhoods, license plate readers were used to double our public transportation lines and unweave our car-tangled cities?

What if “smart city” cameras were used to identify spaces for public rest, placemaking, and needle exchange sites?

What if we had a right to our own bodies and movements, so they were never monitored without a radical and consenting yes?

What if dismantling the bricks of the panopticon, lets us lay a new path to abolition?

## CHAPTER 5: The Age of the Robot Farmer

*“It's more of a good thing.”*

*Monsanto's tagline for the newly created Beneforté, a genetic broccoli variant that the company created, boasted having more nutrients than ever before, and can even actively prevent cancer.*

*For a farmer in northern California whose livelihood depends on the superfood, anything that will help increase the demand feels like good news; especially if they experienced some of the difficulties that have followed other farmers around the country in recent years.*

*Things like not being able to fix their own tractor when it breaks, or face being sued by the manufacturer; wrestling with the decision to keep hired farm workers on for the next year or to switch to a robotic harvester; or being told that the digital information about their own land doesn't belong to them; or battling back the Roundup resistant weed that have grown out of control in an ever-competing who can out battle who between herbicides and disrupted ecosystems.*

*Maybe this specific farmer has a fiance who inherited the farm early, after their father and older sibling both were overtaken by cancer. The tri-folded flag that honors the father's service in Vietnam sits neatly framed in glass and stained pine in the front room. A small condolence from the military after sending home Agent Orange clinging to every cell it could in the father's body.*

*The farmer and their fiance will soon realize the cruel gift — that they are growing a thriving new crop that can help fight cancer, produced by the same company that designed, brewed, barreled, and named the cancer that took their own.*

***

The end of the harvesting season was getting closer and colder.

As some fields were already tucked beneath fresh cover crops, others were filled with root vegetables waiting to be unearthed. Soon, thousands of pounds of potatoes and carrots would need to be pulled up, washed, and cured for the winter.

Samuel Oslund, a farmer in Quebec, recalled what prepping the harvest was like the year before — using a hard bristled brush, scrubbing each piece of produce by hand under the stream of a cold running spigot.

He wrung his hands together, his bones feeling the memory of the freezing water. Hand washing thousands of pounds of crops just wasn't possible anymore.

Oslund started shopping for some kind of tech that could clean the entire harvest at once. The right tool existed, but the price tag was double what he hoped.

He wondered if he could build something similar on his own, maybe find some DIY plans, or enlist the help of a friend or two. While rifling through the internet for a schematic to use as a starting point, he came across a website called FarmHack that would lead him to an eye-opening experience.

Oslund found precisely what he was looking for. A farmer who had the same problem built something that was simple but efficient. In the photo it looked like a large wooden barrel laid on its side, like some kind of Flintstones-esque washing machine about the size of a compact car. The slats of wood had spaces between them, like a whiskey barrel that had come loose. The whole thing had several bands wrapped around it that moved with the assistance of a motor.

After reviewing the plans, he felt he could handle the woodworking side of things but decided to call in backup from his friend Ried for the electric work. After talking about the

project to other farmers for a while, the two found that others nearby needed something similar. They decided to build 14 root washers at once.

The morning of the build, Ried found donated motors and the space to physically put everything together, since assembling them on the farm proved to be too muddy. Dozens of farmers carried armfuls of tools and hardware across the parking lot of a local university. Oslund had stayed up the night before making pots of chili for everyone to share.

The group came together like an assembly line — each person adding their own small adjustment and designated piece. By the end of the day, they built all 14 and then disassembled them into small enough pieces to fit into the trucks and cars, packed to the gills and bouncing down the road to their prospective farms.

The reason why Oslund and so many farmers like him are drafting, sharing, and creating these DIY-open-sourced pieces of agricultural technology is simple — there aren't many other options.

The tech and tools found on farms are rapidly changing. Most of it is created for industrial-sized projects and the big mono-crop farmers.

Smaller scale farms, like Oslund's, are usually ignored — despite accounting for the lion's share of the world's food supply.

The DIY nature of tools like Oslund's root washer is the antithesis of how technology is snowballing on the industrial farm. Today, the technology on a large farm is far more than tractors and combines. AI programs gather data from sensors in the ground, telling a farmer when to plant. Drones, data sensors, and DoorDash are all a part of a new field called digital agriculture — which is a delicately swinging scale when we consider whether a just transition can exist for the surveillance economy and the digital city.

Digital agriculture lies at a complicated crossroads between environmental, labor, and data rights. We can follow a single crop through the agrifood value chain to grasp just how vast digital agriculture's impact really is. Say a farmer in the Midwest grows wheat. That wheat seed may be genetically engineered using ‘biodigital’ data-design platforms, and the wheat itself planted using a self-driving tractor and monitored by soil sensors, which actively gather data about the crop and land. The wheat is then harvested, sold, and made into feed for algorithmically-managed industrial livestock or perhaps ground to flour — all assisted by various digital tools. That flour is again purchased and made into AI-designed fake meats or a hamburger bun — possibly by robots in a digitally controlled food factory. Eventually, that bun sits in a warehouse until it is ordered by a restaurant, likely using a digital ordering system. The bun is then neatly placed on top of the burger you order from DoorDash — the app hundreds of people in your area use to order their dinner. Eventually, that delivery might come from self-driving robot delivery systems.

In 2022, a European farm technology company introduced the world to a massive robot programmed to do a delicate task — individually harvest strawberries. Picking fruit can be fragile, especially when it comes to easily damaged produce like berries. This is why until recently, most fruit is harvested by actual people, farm workers, bending low and pulling back tufts of leaves to reveal ripe fruit.

So it was truly remarkable when a company called Agrobot rolled out a machine that could harvest an entire field of berries without a single soul present. A spider of mechanical arms

extending from the underbelly of a large tractor twists and bends to clip, grab, and drop each berry into a collection bin as it rolls through rows of strawberries.

In 2021 a company called Carbon Robotics introduced an Autonomous LaserWeeder. A large square vehicle rolls through fields, constantly scanning the front, back, and underside with cameras. Those cameras feed the image through an AI algorithm that assesses which plants are crops and which ones are weeds. A flashing white light pulses from under the large vehicle. The light is actually a targeted laser that burns away the weed, like microsurgery. The autonomous weeded is not yet available for purchase but is cueing up its marketing campaigns to hit the market.

What makes both of these hefty pieces of machinery possible is AI. Harvesting and weeding done through the guide of AI is just a tiny taste of how technology is finding its way into even the most intricate farming practices; and where it will further develop.

Digital agriculture is not limited to futuristic robots harvesting crops or mechanical arms tucking seeds into the earth. Digital agriculture can also mean offering cloud services to farm companies for data storage and processing — after all, the data that is collected from farmers and along the food value chain is vast. At its core, digital agriculture is the interweaving of technology into the production, consumption, and control of our food.

The agrifood value chain is increasingly integrated with digital technology, at each step, a lot of information, or data, can be gathered, processed, and used. By redesigning tractors, planters, etc., to have IoT (internet of Things) sensors, it's easy to gather data along the way. Digital agriculture tech can tell a farmer when to plant, power the equipment that processes food, then nudge a consumer to order something specific for dinner. The insight that can be gathered through the entire food value chain is beyond measure. And as climate change continues to

impact food supplies, digital agriculture is an ever-profiting industry, from fertilizer to food ordering apps.

Digital agriculture is intimately woven into our daily lives, and growing fervently. Tech on the farm touches many areas, but the joystick is in the hands of just a few companies. According to a 2022 report by ETC, a research non-profit that "monitors the impact of emerging technologies and corporate strategies on biodiversity, agriculture, and human rights," just four to six dominant firms control most of the industrial food chain. Corporate consolidation is one of the ominous avalanches falling from digital agriculture. The "big 5" of tech (Google, Amazon, Meta, Apple, and Microsoft) are no exception.

Tech giants, like the "big 5," are investing heavily in farming, food production, and delivery. Their hope is to press their digital footholds into the food industry. Microsoft has made extensive agreements with Bayer (formerly Monsanto), national agriculture ministries, and other big agribusiness players. In 2020, Google pledged to invest $10 billion in India over the next five to seven years to help the country adopt more digital technologies in its food systems. Amazon acquired Whole Foods and has invested more than $500 million in food stock. Amazon Web Service (AWS) now creates precision agriculture technology that runs through IoT sensors and soil monitoring systems for farmers.

Two of the top five tech companies (Microsoft and Amazon) are publicly focusing not just on the newest phone or self-driving car but on how our food is grown, processed, and consumed.

If you open Google and search for “digital agriculture,” some of the first things you will see are phrases like “new frontier” and “opportunity.” Near the top of the page is a dropdown list of benefits. Things like reliable management, and insights into crop production — both of which would help a farmer get more out of each harvest. At first glance, digital agriculture seems to be the next wave of technology ready to improve how we connect with the earth and increase food production.

But what do these benefits really mean?

The initial rose-colored hue around digital agriculture is no accident. Google and other large technology companies want to show an idyllic picture of digital agriculture. However, every claim has a thumb on the scale when measured. In reality, this kind of technology has a complicated aftershock socially, environmentally, and economically. What is concerning is when only one perspective is widely shared. There is a broader impact of new technologies and how they often have dire consequences on natural ecosystems and can harm poor rural communities.

One of the concerns for food sovereignty activists is the unbridled power that just a few companies will have over the entire food system when they gather and control agricultural data. Also, the list of companies considered “big players” in this space keeps getting smaller as more companies merge. Four firms, Bayer (Monsanto), Corteva ( Dow+DuPont), BASF, and Syngenta, currently control over half the world’s commercial seed and almost two-thirds of the global pesticide business. Corporate consolidation guts competition, the democratic process, and, in this case, the biodiversity of seeds. Digitization developments are supercharging that consolidation.

One of the methods for this volume of corporate control is data collection. A perfect example of how precision agriculture technology is gathering massive amounts of data is Bayer's Climate Field View technology which uses seed genetics, soil sensors, and tractor monitoring to create a single view for farmers to understand their land and crops. However, Bayer uses this information in the aggregate to tailor their products, guaranteeing production and tying farmers into lengthy contracts. Under some 'outcome-based pricing' arrangements, if the crops get a higher price at the market than expected, Bayer takes a portion of the profits — up to 50%, as noted by one report.

Data on its own is useless without the social quantification sector — the ability to generate, capture, and analyze data. One of the ways this is done is through the IoT sensors, an intersection between hardware and software through sensors attached to devices. These devices could range from tractors to home appliances or Amazon's Echo. According to authors Nick Couldray and Ulises Mejias, the number of connected devices will skyrocket from 27 billion in 2017 to 125 billion by 2030. The real profit of this data steps onto the stage with two players — data analytics firms and data brokerage firms. The end goal of both is the surveillance, analysis, and sale of people's behavior. Couldray and Mejais put it well in their book *The Costs of Connection,* "digital platforms give gatekeeping power to their owners, much as the navigation routes of historical colonialism empowered the towns near where goods had to land."

Agriculture and food data is becoming more and more valuable. When we gather massive amounts of data along the entire agrifood value chain, that information becomes a goldmine for tech and agricultural companies to maximize their tech to make as much money as possible or sell that data to data brokers. This was why the CEO of Monsanto (now Bayer), Rob Fraley, noted in 2013 that "I could easily see us in the next five or ten years being an information

technology company." In fact, that is exactly what happened. The power of farm, ecological, and consumer data allows corporations to control the end-to-end production of food and creates a new revenue stream.

Agricultural data can provide farmers with valuable insight into crops and livestock. Access to that information is alluring for many farmers. While the benefits of precision agriculture are accurate, there are hidden costs. One of which is the data that precision agriculture collects, farmers typically are not allowed to own even though it comes from their land. Still, like anything of value, data can be used to further the profits of some or the collective knowledge of all. Data is becoming the new oil with rising value and vast reserves quickly emerging.

Not all digital agriculture is bad. The insights that can be gathered from IoT sensors, food production facilities, and even traffic patterns from an Uber Eats driver, could be used to better cope with a changing climate. Ideally, these insights could help make our food systems more resilient when faced with disruption. Digital agriculture as a force for good might look like solar punk movements. The term "solar punk" began in 2008 and has since snowballed to mean shifts in design that center ecology and human technology living in coexistence — imagine an urban farm that uses IoT sensors to monitor soil health, while trading their produce with neighbors nearby. It's a small ecological footprint that is made more resilient through technology.

Many large companies that are proponents of digital agriculture try to say issues like climate change, world hunger, and better working conditions are all ripple effects when more people use digital agriculture. Tech companies are eager to share ways digital agriculture can solve economic and ecological problems. Microsoft believes FarmBeats — a farm sensor, drone,

and machine learning algorithm tool — is how farmers will be able to amp up production to feed twice as many people by 2050, for example. The list of benefits that tech companies typically cite is often reused over and over. Things like: robots will save farmers from back-breaking labor; precision agriculture can help soften the blow of industrial agriculture on the environment; data insights will lead to higher crop yields, thus helping address world hunger; and more buying options can meet the needs of consumers.

The tech behind digital agriculture often looks like a magic wand — with one wave, significant contributors to climate change fade while simultaneously halting a looming hunger crisis. This narrative is actually not without a foothold; there are serious concerns about how our present-day agriculture will evolve alongside a changing planet. The UN and other international research entities warn us about the ever-strengthening bond between global food security and climate change. Food systems are threatened by degrading ecosystems, and unsustainable industrial farming is no minor contributor to greenhouse gasses. The EPA estimates that agriculture accounted for 11.2 percent of U.S. greenhouse gas emissions in 2020.

Environmental groups often hear that digital agriculture is a golden-one-way ticket to regenerative farming, carbon reduction, and a tap into the lucrative world of carbon credits. Big tech companies often frame digital agriculture as a way to make food systems more resilient against disruptions like pandemics. In one of ETC's recent reports, they note that "in 2020, the U.K. Research and Innovation agency awarded £2.5 million to a consortium of academic and private sector firms developing the world's first robotic farm, dubbed 'Robot Highways.' The project claims that its autonomous tech will enable a 40 percent reduction in labor and help move the sector toward a carbon zero future."

The idea is that if we improve efficiency, the problem is solved. This isn't exactly true according to Samir Doshi, a scholar who studies race and technology. Doshi points out Jevons Paradox — a concept from the energy sector. Jevons Paradox states if energy is produced more efficiently, carbon emissions will not fall, unlike most assumptions. He notes roughly 40 years of data show this paradox to be true. "Years of data show that even though you might increase the energy efficiency of a household or residence you're still increasing consumption," says Doshi. "So you actually don't reduce consumption overall. You're still increasing it. You're just having a more efficient means of increasing it."

Researchers with civil society groups are concerned that many digital agriculture claims are built on assumptions or, worse, are creating problems that do not exist. The World Economic Forum notes that if 15 to 20 percent of farms adopt precision agriculture, it could increase global yields by 15 to 20 percent. The World Economic Forum goes on to say that precision agriculture could decrease greenhouse gas, emissions, and water by 10 to 20 percent on top of that. EPA estimates that agriculture accounted for 11.2 percent of U.S. greenhouse gas emissions in 2020. However, greenhouse gasses are not the only measurement of environmental health. Industrial agriculture greatly contributes to freshwater use, pollution, and soil erosion.

The basis of this symbiotic argument — that food systems will adversely harm the environment and that agriculture is a massive contribution to climate change — assumes that our current food system remains unchanged. Yes, on the current course of climate change and industrial agriculture, both will continue in a cause-and-effect cycle with one another.

Caddy corner to environmental discussions, one of the common justifications for digital agriculture is population growth. Many proponents say that by 2050, Earth will be home to 10 billion people. Therefore we won't have enough food, much less means of food production that

isn't destroying ecosystems. In theory, we would need to increase food production anywhere from 50 to 70 percent to supply that many additional people on the planet. Tech companies often claim that digital technologies are a way to feed a starving future.

Similar to the narrative distortion of digital agriculture and climate change or solving world hunger, farmers often hear that the more technology they implement the fewer workers they will need on the farm — which is true. The hidden cost of that truth is many farmers then become dependent on the brands of tech they are using and the connected products. Certain planters only work with certain seeds, etc.

Some farmers are now part of a growing movement known as the "right to repair." Machinery companies like John Deere state that when someone buys a tractor, they are given a "license to operate the vehicle," but are not actually the owner of it; nor does the farmer own any of the software it comes with or the data that the tractor generates. Right to repair essentially asserts that if a farmer owns a tractor, they should have the right to at least be able to work on that machinery — seems a no-brainer.

There is, however, immense danger in farmers not owning their data or being able to work on their own equipment. For anyone working with farmers daily, figuring out whether to use the technology presented to them is difficult. On the one hand, farmers need to keep up with competition and maintain their livelihoods; using the newest technology to improve crop yields or scale-up production is enticing. On the other hand, by becoming dependent on big tech, farmers are tying themselves to large corporations for the long haul. The degree of corporate reach and control on the farm quickly pulls autonomy away from those working with the land.

Not having the right to work on your equipment violates an owner's autonomy and can be considered a labor rights issue. When digital agriculture is rolled out on farms, one of the immediate impacts is on laborers, the people who help plant, pick, and maintain crops or livestock. The majority of these workers are BIPOC. According to the USDA, only 24 percent of crop laborers are white. Digital agriculture swings the hammer, starting a Rube Goldberg chain of reactions touching racism and labor rights.

When automation tools were introduced to coal mining, the technology was presented as beneficial, because automated machines would prevent miners from having to spend as long breathing in silica dust. Instead of black lung disease, miners and their families faced wide-scale pollution that coated the ecosystems from amping up coal production. Health and safety were never a metric to start with — instead technological advances often substitute one health issue for another.

The honey trap of digital agriculture is it creates the tools that make industrial farming possible — contributing significantly to climate change — then profits again when they offer a surveillance-fueled diagnosis to treat a withering planet.

However, some groups hope to change the narrative and discuss a different future. For many farmers, two issues need addressing; working conditions and developing methods that further the resilience of rural communities.

Those working to chart alternative futures are often anchored by collective problem-solving. Turning to farmer-led innovation addresses many of the issues created along the agrifood value system. By allowing farmers to collaborate and design their own technology, they are creating responsive tech that is suited for their particular ecosystem. If farmers can build

their own technologies, they own and control their data. By not relying heavily on corporations, growers are likely part of smaller farms, also known as peasant food webs. It should be noted that the peasant food web still feeds roughly 70 percent of the planet with far fewer resources — less than 30 percent of the world's land, water, and agriculture. These smaller diverse systems of farming create resilient communities and can play a role in slowing climate change.

Oslund's root washer is a paragon and a glimpse into an alternate future — one of sustainable smaller-scale farming and technology that serves rather than exploits. Small farms are one of many solutions to help address climate change. While technology on the farm can help make smarter choices, those who work with the land need to have a say in the design process. Fueling the planet's destruction while simultaneously profiting from it will be the legacy of industrial digital agriculture unless we intercede. Realistically, changes like this are the best stepping stone to a just transition for digital agriculture.

## CHAPTER 8: The Cities Where Data Counts

*In a universe that splits into infinite branches, down one of those there might be a young man walking down a city street 50 years from now. The street is lined with thick-trunked trees, twisting and craning overhead.*

*Maybe in this future there is a piece of tech in the young man's pocket, something like a thin piece of glass the size of a stick of gum. He pulls it out and holds it in parallel to the ground, turning on a small*

*projection that looks like a clearer version of the holograms he would see in classic movies. Maybe this tech is programed with a deepfake AI of his grandmother.*

*"Look it's your trees!" he says to the hologram, a bust of his late maternal grandmother.*

*The AI sorts through thousands of videos of the grandmother and uses her writing to generate a response that sounds like something she would say.*

*"Well, would you look at that. How are my baby blues doing?" she asked, meaning the Chicago Blues aka Black Locust trees that she helped to plant years ago.*

*In this future, the grandmother might be one of the many people who could have taken advantage of the open sourced sensors and IoT devices throughout the city. She would have used them to find urban heat islands and start a business to plant trees in those neighborhoods.*

*In that future, the young man smiles and begins to describe the dripping white blossoms as he walks further down the street, every step in the shade.*

***

Data is the true leviathan swimming under the technology of "smart." Smart cities can make life simpler in many ways, but the cost of that ease is the same current that connects it — and when there are vast amounts of data being produced, there also needs to be wise people who decide what to do with it.

How to build sustainable data management is one of the biggest challenges today for digital rights organizations.

Sidewalk Labs is yet again another interesting case study. One of the primary concerns about the project came from those who were worried about the residents' privacy. The concerns were warranted. Not only was Sidewalk Labs hoping to gather data about transit, foot traffic, air

quality, and waste, it also planned to install “urban USB ports” around the neighborhood that would allow other companies to easily install sensors and gather additional data, according to CNN.

The idea gave an open door to civil society groups and Toronto residents who had questions.

What would happen with all the data and information that was collected? Where would it go? Would it be sold to some nefarious corporation? Would it be used to monitor and track the residents?

The sheer amount of data from this specific space would likely be rather valuable since it would be so thorough and well documented. If this were the case, then would residents see a percentage of the profit? How could someone request to have their data removed entirely? Was it even possible?

Sidewalk Labs came up with a solution that the group coined as “the Urban Data Trust.” The idea was to create some transparency into what would happen with the data after it was collected. Other methods for data governance — like opting into data that was gathered consensually, like by understanding and signing a form — aren’t exactly possible with an openly accessible space. Deciding how data governance will work is one of the ongoing challenges in smart city design.

The Urban Data Trust suggested that Toronto’s smart city data would be housed and regulated by an outside trust with folks from a variety of industries and backgrounds serving as the trustees. Harvard Business Review explains that a data trust is set up so that the trustees represent the data providers, deciding whether their data gets sold to another company or making

legal decisions about the data itself. One of the issues with Sidewalk Lab's plan was that there weren't enough specifics to make the trust a sound idea. The plan never noted what nonprofit would oversee the data trust or how the trustee members would be selected.

Smart city data collection holds a particular challenge for data trusts because there is such a diverse mix of data — transit, water, utilities, etc. It's difficult to decide who has access to it when there are so many stakeholders and they all find different things valuable. Proponents of data trusts often suggest having numerous trusts for different types of data; one for transit data, one for water usage, one for utilities, and so on. Making decisions on what to do with data in one of those areas could be the wrong decision for another.

Data scholars like Anna Artyushina, have found that the Urban Data Trust would likely only truly benefit private actors instead of the actual people who live and work in the Toronto neighborhood. One of Artyushina's research papers note that the design of the trust itself is meant to make it easier for private companies to collect, reuse, and profit from it.

The trust that Sidewalk Labs proposed introduced a new legal definition for data that would allow the trust to maintain control over it entirely. The question of 'who owns data' is one of the recurring points made by big tech — since it is in big tech's best interest to stoke the fire under that question, fanning the flame for more debate while in the meantime, they are able to rapidly gather as much information as possible before any kind of well-forged answer emerges.

The idea of a data trust in this scenario misses the mark in many ways. One of which occurs well before any piece of data reaches a server and even before the first construction signs are unloaded off the bed of a truck. The process of retrofitting a city with data-tracking devices sets up a space where the company installing them can easily (and likely) create a closed loop,

giving it a monopoly on what new pieces of tech could be integrated into the city. More than that there is the very present disparity between the people who live near this part of Toronto and who could afford to live there once something like Sidewalk Labs transformed the area. Artyushina notes that the Urban Data Trust is "a cautionary tale that demonstrates that treating data as an asset may expose even civic projects to the threats of a rentiership economy."

Perhaps most concerning in all the Sidewalk Lab plans, is the gatekeeping that comes with access to the area. If a resident did not want to be tracked and monitored, they could opt out, but doing so would mean that they wouldn't be able to use many services in the city. Josh O'Kane, author of the book *Sideways: The City Google Couldn't Buy,* shares a concealed document called The Yellow Book, a 437-page document with Sidewalk Lab's notes on "a city from the internet up." One of the most notable parts of The Yellow Book was the way data was talked about almost as a currency — where without providing it, people wouldn't have access to certain aspects of the city.

Residents can opt out if they want to, but to do so is nearly impossible if they want to move through their day easily… sound familiar? Today, yes a user could opt out of data collection but to do so means that they don't have access to the things that make the day-to-day easier. Things like online banking, navigation from a phone, the ability to reply quickly to a work email, or finding out when an event is happening down the block. Not using technology that tracks and monitors is no longer an option.

Sidewalk Labs referring to data as currency is an ill-placed metaphor. Calling data currency makes it seem like a resident has to earn the right to be in a space, and that they need to

work for access to common spaces. Well-designed cities are a tapestry of spaces meant to be a public good.

Calling data currency frames data as something that corporations and banks essentially loan out in exchange for work — but in the end, it belongs to them.

Calling data currency makes it seem like the more residents offer up, the more they will have and the happier they will be.

Calling data currency changes it from information that could be open, accessible, and transformative to something that capitalism already has a well-established system to gather and hold on to it.

Privatized smart city technology inevitably leads to data rentiership.

Rentiership is a fascinating way to think about data and how it impacts urban landscapes. The word, of course, comes from renting property, or something valuable, to someone else. Rentiership, though, speaks to retiership capitalism — a system that seals a foundation for the building of a bourgeoisie. Rentier capitalism is an extraction of resources without contributing to an ecosystem in return; it is class violence.

Take the example of housing. A landlord buys up 20 houses around a city. He then applies a few cosmetic changes and rents the homes out, charging three times what the mortgage would be. Planet Starbucks circles around the corner and changes the tide. The neighborhood slowly gentrifies. Renting is the process of amassing wealth by creating an enclosure around

something. In this moment the landlord becomes part of a larger process, one where he creates an artificial scarcity of housing by limiting who can afford to be there.

Vladimir Lenin referred to rentership as a “seal of parasitism” that feeds off exploiting the labor of other countries. In the case of data, this is particularly true. When big tech collects information about people’s movements, daily patterns, interactions with the environment around them, spending habits, feelings, and even goals, it isn’t gathering something that it helped create, it is selling an observation. Those observations are in many ways used to exploit the same communities that created them in the first place. Big tech calls surveillance its labor and data a wild food that it foraged. In reality, big data is taking part in rentiership capitalism — putting a wall around something that should be a public good and calling it theirs.

Another way to think of rentiership is through the image of a lease. Renting is putting a limitation on the amount of time that someone else can hold on to something — paying for the feeling of autonomy without the reward. In the case of data rentiership, big tech allows us to feel like we have autonomy over our environments through the control we feel with smart technology while paying for it with our privacy.

One of Artyushina’s research points to a strong connection between “the privatization of city administration in smart cities and the emergence of data rentiership as a governance model.” There is a difficult challenge for those who see the potential benefit of smart city technology but don’t want to create a system of data rentiership. Can you create a smart city without surveillance and extraction?

A few have tried, but Barcelona succeeded.

***

Barcelona is one of the few smart cities in the world to be making steps toward sustainability while preserving the rights of those who live there. Barcelona has been seen as the shining beacon of smart cities. The technology of IoT sensors, cameras, microphones, aggregated data from transportation, energy usage, and even irrigation are all woven together into a smart city grid. The tech all works together to gather data about the movement and sustainability of the city. That data is shared with the government and private companies — which sounds like a red flag. And it was for residents.

Which is why back in 2015, Ada Colau was named mayor of Barcelona despite having no government experience.

Colau was Barcelona's first woman to be elected mayor and came from feminist and revolutionary movements before her. Colau was also part of a political organization called Barcelona en Comú, or "Barcelona in Common" in Catalan. The group referred to itself as a platform instead of a political party, inviting participatory decision making at every level.

In order to understand Barcelona en Comú, traveling 1,035 kilometers north to Paris and rewinding to 144 years into the past is a necessary prerequisite. Barcelona en Comú drew their ideology from a movement known as Commune de Paris, or The Paris Commune.

The Paris Commune political movement is most well known for seizing power in Paris for just two months in 1871, nearly a hundred years after the French Revolution. However, in

those two months the radical leftist revolutionaries made sweeping changes to a city that was under the thumb of the bourgeoisie and the church.

The Paris Commune was known for radical feminist leaders and progressive ideology. The group fought its way to power and while it was in control of the city ended cruel policies and established equitable and just systems in its place. The Paris Commune immediately separated the church and the state, eradicated the exploitation of children as a labor force, set up systems of self-policing, cut back on rentiership, and even empowered employees to seize control of a business if the owner was not present for long periods of time. The movement cut off the blood supply for elite systems of power that exploited workers and the majority of the city. The Paris Commune was such a powerful movement, it directly snowballed into the writings, critiques, and concepts from Marx and Lenin — both of whom said the Paris Commune was on the right track but didn't do enough to hold their position in the city. The Paris Commune alas did not hold that position for long at all. At the end of the two months the French military swept through the city, killing somewhere between 10,000 and 20,000 people who were standing with The Commune.

The collective action and fervent focus on democratic systems were mirrored years later in Barcelona. Barcelona en Comú organized and voted in members of the group into the majority in city hall. The group had ambitious plans to address issues in Barcelona like improving access to education, equitable housing practices, more efficient and environmentally sound transit, improving access to food, and work toward water sustainability. All of these were near perfect, modernized reflections of The Paris Commune.

Barcelona en Comú organized and saw the potential behind smart cities and the duality of their potential harm if mismanaged. In order to set up better data practices and dismantle a spreading digital panopticon surveillance system, Barcelona en Comú would need to be in a position of power to guide the extractive smart city toward a sustainable digital city.

Being in the majority of city hall allowed Barcelona en Comú to select a mayor — former housing activist Colau was the obvious choice. Within the next five years, Barcelona en Comú made public services education, housing, transit, food, and water either cheap or entirely free. *Dissent* magazine notes that in those five years, public officials were given term limits and barred from assuming positions of supervision in any kind of private company in their sector, real-estate speculators and banks were limited by sanctions, and the data collected from smart city technology had to be approached with open consent from collectors and agency to revoke access to it at any time. *Dissent* magazine also notes that Barcelona en Comú was "able to put a moratorium on new hotel construction, close over 2,000 illegal tourist apartments, sanction Airbnb for illegal establishments, and even begin to expropriate landlords who keep apartments vacant." All of this was in addition to creating the first LGBTQ center run by the city and kickstarting a sustainable public energy company. Today there are additional protections for migrants and anti-eviction regulations in place because of the work of Colau and Barcelona en Comú.

Colau's position of power came at the request of residents who saw her background as a housing activist as an asset to her understanding of smart city technology and a skillset that would help her set up ways to democratize data throughout Barcelona.

Barcelona's new mayor brought in a digital participatory platform, Decidim, meaning "We Decide" in Catalan, as *Wired* notes. Decidim lived up to its name and allowed the people to vote for what they wanted done with this new-found information and insights about their city. The same *Wired* article adds that affordable housing, energy transition, air quality, and the open accessible use of public areas all ranked as top priorities amongst the voters. The city listened to the requests and has since directed more funds and projects to address them. Barcelona's Chief Technology and Digital Innovation Officer, Francesca Bria, told *Wired, "*we want to move from a model of surveillance capitalism, where data is opaque and not transparent, to a model where citizens themselves can own the data."

The shift that Bria and Colau ushered in changed the flow of data in Barcelona — the undercurrent of their ideas was that data belonged to the citizens of the city.

On a very basic level this meant changing how data was procured in the city. Because the government didn't have the capacity to physically create the technology that was needed or the ability to interpret that data, making sustainable contracts with private entities was a necessary step. The shift in perspective though made it easy for the new city leadership to ensure that new contracts had considerations like data sovereignty and strict regulation on what could be done with the data once a private entity had it. A small example is Vodafone, a UK telecom company that set up cameras to monitor traffic patterns in Barcelona. Vodafone had to share all that data with the government and had restraints on how they could use it.

A much larger project was the creation of Project DECODE — which stood for Decentralised Citizen-owned Data Ecosystems. DECODE allowed citizens to have complete

control over their data. They can decide things like what kind of data they want to share, what should be kept private, who can see it, who can share it, and what they can do with it.

Another part of DECODE in Barcelona allowed citizens to place sensors where they wanted — collecting encrypted and anonymous data on things like noise levels and pollution. DECODE also taught people how to set up the sensors, monitor them, and analyze the data if they wanted to. The idea was to allow folks to use this information about their own neighborhoods when they made requests through Decidim.

The DECODE project ran from 2017 to 2019 and was also used in Amerstam, another urban space that has ample smart city technology. Project DECODE effectively brought the first stages of a consensual smart city to Barcelona and set it down the path of data feminism as its headwater.

Cities allowing private companies to gather the data of its citizens, though, can lead to its fair share of concerns. These companies control a vast amount of data. And this data is not only used to provide the service that it is offering, but it is also sold off to other companies for a profit — and how that data is used by the recipient is entirely out of the initial company (and the given city government's) control.

What if smart homes also limit access to information? A step further, what does that mean when the government can listen through smart home devices to find indications of what they call child abuse but is really trans people just living their lives? What happens when someone types the location of an abortion clinic into the navigation of a smart car? What happens when frightening legislation passes and the "smart" tech is deputized as an extension of the police?

While smart homes depend on a desire for convenience, smart cities depend on a lack of dreaming. When the city stops dreaming up new ways of being, its citizens let go of the possibility of ecotopia. Instead they accept surveillance dressed up as sustainability.

***

In Indianapolis there is a neighborhood just north of Indiana Avenue, a street that is known for being a plaza of Black wealth and art in the first half of the twentieth century. The Avenue used to swell and sweat with live music; jazz legends like Duke Ellington, Cab Calloway, Ella Fitzgerald, Hampton Sisters, and Wes Montgomery performed there often. The neighborhood north of the Avenue was home to Madame C.J. Walker, the first female self-made millionaire in America, who built her business empire through salons and hair care products specializing in Black hair.

A few blocks away from Madame C.J. Walker's house and fast forward a little over a century later, Carlette Duffy was trying to get her home appraised. Carlette went through the process twice and both times she felt like she was being low balled. Especially considering the neighborhood was going up in value, sat a few blocks away from luxury townhouses along the canal, and was a short walk away from a large university and one of the nicer hospitals. Everything in her gut said she should be getting a higher number from the bank.

She suspected that the low appraisal was because she is Black. She decided to test the theory. Yet again she submitted an application for appraisal, changing nothing about it except this time she concealed her race. Her home went from $125,000 and $110,000 the first round, then

shot up to $259,000 when the mortgage lenders didn't know she was Black. Today, she has filed fair housing complaints against the mortgage lenders and appraisers.

Carlette is not alone, and her story is proof of the bias that is built into the algorithms of cities today. What Carlette experienced is a small sector of digital redlining.

Digital redlining, of course, harkens back to the practice of redlining — when banks would deny home loan applications based on neighborhoods that they deemed to be "in the red." Maps were created that color coded neighborhoods as either green, yellow, or red — on paper these noted "risk" levels of lending to folks in each area. In actuality, being in a red zone simply meant most of the residents were Black.

Digital redlining is a broad term, describing problems that can only be considered related as cousins at best. Digital redlining can mean a few different things. It can refer to a lack of broadband internet access in a poor area, often where BIPOC folks live who have historically been segregated by redlining. Digital redlining can also refer to the racist data that has become mixed into the foundation of many algorithms. This is one of the main concerns with AI — if the base algorithm that is duplicated over and over has racist data built into its DNA, then it will repeat those racist decisions time and again.

Language is important here, so pausing to acknowledge the racially specific pain that comes with using a word like "redlining" to describe access to the internet. Some might, and could be right in pointing out that having access to housing and the chance at generational wealth is not nearly the same as having access to the internet. On the other hand the value of internet access is arguably a human rights, as proven through COVID.

The phrase “digital redlining” is used almost in the same manner that some folks in the ecojustice world use words like apartheid — connoting a specific time and a racist act that was, and is, tied to place. Both words however have an entirely different meaning for those impacted by the originating acts. The families who experienced the murder and destruction in South Africa and the family who fought tooth and nail to buy a home only to have the line for generational wealth moved just out of reach year after year by the bank — neither are respected when we refer to digital redlining without acknowledging the pain and generational trauma of institutional racism.

Now to bring the history to the digital present.

The discriminatory practice of redlining became the model for how cities rapidly expanded in the 1900’s. Once the practice of redlining was in place it impacted generations to come, snowballing into self-fulling prophecies about education, crime, and health. The data collected from redlined neighborhoods became a part of housing predictions. It became part of financial data models. It even became the reason why cities didn’t plant as many trees in Black neighborhoods — and why today those areas have higher heat indexes, are less likely to be resilient to climate change, and why the utilities cost more. Redlining became an invasive species that continues to change the ecosystem of cities today despite it being illegal since 1960.

Detroit is the case study on how digital redlining has impacted access to the internet. It is estimated that 70 percent of school aged kids don’t have access to the internet in Detroit, according to the University of Michigan. The Hill reported that 40 percent of homes in Detroit don’t have any kind of internet access. In 2017, the National Digital Inclusion Alliance found

that AT&T chose not to install newer fiber technology — that would bring high speed internet access along with it — to neighborhoods that had a poverty rate of 35 percent or more. This systemic refusal for access is digital redlining.

Detroit is by no means the only city finding digital redlining in its infrastructure. The Electronic Frontier Foundation notes that areas like Oakland and Los Angeles County have both demonstrated systemic discrimination against low-income neighborhoods, something that is easily seen in the fiber deployment compared to high population density. AT&T again was found to be particularly at fault. A study by the Communications Workers of America and National Digital Inclusion Alliance found that this digital redlining is systemic in the company's practices.

Digital redlining can also be the practice of unfair ad-targeting, and is the subject of several ACLU cases. The common thread between them is the social media companies using a users' zip code, race, and gender as reasons to not show them certain ads that had things like housing deals, credit lines, or job postings. The ACLU is still advocating for these cases, saying that the same kinds of discrimination that are illegal should apply to digital spaces too. The use of discriminatory online ad-targeting can replicate institutional racism — thus excluding people who are historically marginalized from access to basic human rights like housing.

Sadly, bias is built into the core of our tech. This might look like the algorithms that a fintech company uses when it determines what rate you might pay on insurance, or if you qualify for a loan, or how long that loan is — all based on preexisting information that is often part of our tech and fine tuned using our internet data. Roughly 56% of fintech startups use AI in at least one aspect of business, the most common is in risk management.

Take the example of Kevin Johnson, who in 2008 became known for having his credit card limit dropped by $7,000. The reason, according to American Express, was that he was shopping at a Walmart where many shoppers had a poor repayment history. This level of digital surveillance was quickly rebuked by American Express and their policies changed to conceal them better.

Today, data surveillance has only increased, and with it so has predatory lending practices and police surveillance. These practices are connected to digital redlining in many ways and many know these problems exist but are not sure what to do. The FCC is even creating a task force that has to come up with rules by November 2023 to address digital redlining by broadband companies.

In late 2023, the Biden administration released a lengthy guideline on AI, and a direct portion of it tied to digital redlining. According to CBS the administration is attempting to set up barriers to prevent banks from using algorithms that make loan decisions using data that continues the reach of redlining into a fully automated and instant decision on who is approved or denied for a loan. The guidance from the Biden administration will start requiring tech companies who develop AI to report on how it's created and to monitor and fix biases that are baked into the data sets. Whether this will end up being too little too late or a powerful first step is unclear. Biden's order extends to algorithms used in health care and law enforcement — all in the hopes of spotting potential discrimination before it spreads too far.

There are, however, alternatives and even paths where systemic oppression and the data that came from it, can be used for good. In California, the state developed an algorithm to decide where to invest the money from carbon taxes, which is in the millions. They use the same terms

and algorithms that banks have used to *deny* loans to identify areas that needed more support. This effort built parks, affordable housing, electric vehicle charging stations, and even planted trees in neighborhoods that desperately needed it.

Sometimes the master's tools can at least loosen a few bolts and nails that hold the master's house together.

The way that tech and the city integrate with one another has the cause and effect relationship of an ecosystem. One changes and the other evolves in response. However, when the symbiotic relationship between the city and tech changes too quickly — sidestepping evaluation and intersectional intentionality — institutional hatred becomes bred into the DNA of each iteration.