
UNDER
SURVEILLANCE
C:\Users\quinn>TYPE Panopticon.txt
Vol 2: Capstone

Section 1: Cameras

New York City is infested with surveillance technology. It seeps under our door frames and runs down our blocks, pooling in the subways. It is pervasive, it is pernicious, and it is largely invisible. Thousands of little digital eyes watch us as we walk down the street.

The first and probably most visible instance of surveillance technology is the network of cameras that litter neighborhoods throughout the city. How many cameras are on your block? I count 8 on mine, and those are just the ones I can see. Hidden cameras are very common in New York. If a door looks like it has two peepholes, there's a good chance one of them is actually a camera lens. Cameras are often hidden behind mirrors, or disguised as pipes. These can be spotted if you're paying attention to the ceiling next time you ride the subway. The ownership of these cameras varies, some held by companies, some by landlords, and some by the government.

Government cameras include red-light cameras, speed cameras, license plate cameras, and live video cameras. Some of these cameras can be located here. There have been other attempts to map the cameras around New York, but the accuracy of these maps is questionable. Firstly, because as mentioned, many of the cameras are invisible to the naked eye. New York is not a corpse however; it breathes and grows and changes. It changes quickly enough that a map of cameras made a couple years ago bears little resemblance to the current landscape. These documents then, are more useful as a snapshot of history, than for any kind of pathfinding.

One of these cartographic missions is the NYCLU Surveillance Camera Project. The project was completed in 1998, by a group of NYCLU volunteers, and is available here. Surveillance Camera Players were/are an activist group in New York opposed to Video Surveillance. There are some fascinating videos from early demonstrations up on YouTube, but many of the links died years ago. Their collection of maps is available via the notbored zine's website. The group was part of a global anti-surveillance 'day of action' that happened 4 days before 9-11.

The number of exact cameras in the city varies from source to source, due in part to the ever-changing nature of the city, government opacity, and bureaucratic disarray. An article in Security Today put the number of cameras plugged into the NYPD's Microsoft-backed Domain Awareness System at 2,626 (in oct of 2018), and said the system would grow to include over 18,000 cameras, including private CCTV systems. In 2015,

the New York Daily News put the number of cameras in the NYPD's system at 17,000, 6,000 street cameras, 7,000 in public housing, and 4,000 in the subway. In 2018, the City Council asked for $100 million for more security cameras for schools.

The types of cameras owned and operated by the government vary, with different departments of the New York City government using different cameras and camera systems. The Department of Transportation has live cameras manufactured by the Swedish video company Axis Communications, that hang in intersections around the city. The live feed from most of these cameras is available via the DOT's traffic cam site.

The NYPD has multiple camera networks, one of which is co-owned/operated by the Department of Homeland Security. This is the CrimeEye® system, developed by Total Recall Corporation (TRC). TRC is listed as a Convergint Technologies Company (subsidiary), but it seems to predate its parent company. TRC was incorporated via Corporation Service Company in Albany on November 26, 1985, while Convergint Technologies llc was formed in May of 2002, through the same Corporation Service Company. TRC is based in New York, or at least they still appear to have offices in New York. It's not surprising to see these kinds of intertwining of government and private companies, after all what is neoliberalism if not the reification of the market and privatization of fields previously thought to be public. Details on this specific

TRC project remain scarce, but they have worked with Axis Communications as well as a handful of other multinational companies in the past. he NYPD also has its own camera system, which it calls Argus. This is not to be confused with DARPA's ARGUS-IS project, or the many other security cameras called 'argus'. Argus Panoptes was a giant in greek mythology with a hundred eyes, and camera companies (as well as police departments) are bad at naming things. The NYPD argus cameras are identifiable by their easy-to-spot white housing. The cameras jutting from the side of the enclosure are manufactured by Pelco, a California-based company owned by Motorola Solutions. There is also a wireless transmitter on the top of the box, manufactured by another California Company- Proxim Wireless Corporation.

Hermes killed Argus Panoptes with a rock, after lulling him to sleep with his flute. Does the music in Washington Square park ever make the cameras perched above it tired?

Section 2: Exhaust

Every time you interact with a digital technology, something is produced. What is produced is metadata: data about data. We have complex devices producing heaps of data in every interaction, from 'liking' a post to just having a cellphone in our pocket as we walk around. This exhaust, or "behavioral surplus", and the political economy of it is the focus of Shoshana Zuboff's work: The Age of Surveillance Capitalism. The discovery of this value happened at Google in the late 90s or early 2000s, and was kept secret. Zuboff writes: "What had been regarded as waste material—"data exhaust" spewed into Google's servers during the combustive action of Search—was quickly reimagined as a critical element in the transformation of Google's search engine into a reflexive process of continuous learning and improvement." This surplus was first used solely to improve the product of google search, a process Zuboff calls behavioral value reinvestment cycle, but soon it shifted into surveillance capitalism, where the behavioral surplus is converted into capital through advertising. The newfound profitability of this

surveillance of behavior led to a renaissance in techniques and technologies of its harvest.

One significant infrastructure project for this kind of surveillance is LinkNYC, the ugly steel-glass contraptions that stand on street corners throughout the city. These monstrosities are owned and operated by a conglomerate called CityBridge, including Qualcomm, Titan, and Control Group. Titan, and advertising company, and Control Group, a design firm, were acquired by Alphabet (Google) subsidiary Sidewalk Labs. According to the Village Voice, at the time of its rollout, DeBlasio trumpeted the achievement that the city was getting this infrastructure, with free high-speed internet, for free. However this was not exactly true, in fact SideWalk labs had agreed to pay the city over five hundred million dollars over the next twelve years. If one buys the argument that anything free in New York is suspect, then what are we to make of a company paying for the privilege of giving something away. There was clearly something suspect, as one of the Gimbal, one of the advertisers involved in the product, tried to offer the Voice an under the table deal potentially in violation of New York City advertising ordinances.

The Voice pressed LinkNYC on their privacy policy which left open some enormous holes for tracking and advertising, which LinkNYC said that they of course were not using. In May of 2018, a student at New York City College of Technology, Charles Meyers, discovered codebases in LinkNYCs public github that appeared to be sophisticated tracking algorithms. Myers shared this code with The Intercept. In Myers' view the databases "LinkNYC Mobile Observation" and "RxLocation" seem to collect users location, browser, operating system,

device identifiers, and web use, and aggregates the data into a database. He went on to say that if the code was running on the kiosks, the company would be able to automatically target ads to those walking by. LinkNYC replied by saying that the code was merely a test, and not running on any machines. Technology experts consulted by the Intercept agreed with Meyers on the purpose

of the code, but concluded it was unlikely that it was running on kiosks, due to unfinished chunks of the code. LinkNYC tried to have Myers' copy of the code removed after being contacted by the Intercept, but it is still archived and available here. We know that some amount of surveillance by the machines is happening, as in 2019 video from one kiosk was used to identify the man who was

smashing dozens of the monoliths throughout the west village.

If there is any silver lining to the story of LinkNYC, it is that the project seems to have failed. The company stopped installing new kiosks in 2018, and only materialized a fraction of the total number promised. On top of that the company, according to the City of New York, is delinquent and owes the city millions of dollars.

Some of this tracking apparatus is, of course, redundant, as we carry sophisticated tracking technology in our pockets. The Brennan Center compiled a simplified introduction to how cell tracking works. Cell phones constantly search and try to connect to the closest cell tower. This process has the effect of triangulation of a user's cell device, with an accuracy roughly between a thousand feet, or only a few, depending on the density of cell towers. This is not the 'location services' that uses GPS and can be turned off in the settings of most devices, but the very functioning of the phone itself, and works just as well on devices without GPS installed. This data is called cell site location information (CSLI), and is stored by service providers for up to seven years. Police can access this information with a court order, but if they want more than 7 days of it, they need a warrant. They can also request information about every device that connected to a single tower, rather than every tower contacted by a single device. This lets them identify every cellphone in a given area at a given time, given the cellphone was on. The police also have the ability to 'ping' a cell phone to find it's location using the enhanced 9-11 system, and although the courts have not ruled definitely, consensus seems to support a warrant requirement. Police can also use a device referred to as a stingray, which is essentially a fake cell tower that records all

the phone information in a given area.

These and other similar systems of data collection in urban environments are euphemistically referred to as 'smart city' technologies. Sidewalk Labs, the creators of LinkNYC, also make various other 'smart city' products. These include energy use surveillance, and a panoptic location data collection system in Portland. These projects have been hard hit by the pandemic however. It seems like many so-called 'smart city' projects have shrunk or fragmented, with the S&P projecting at least a 7% fall in 2021, as well as the high profile Cisco project shutting down. That S&P report did project a later growth in these technologies in 2022 through 2024.

These smart cities and mobile technologies are not the only kind of exhaust that can be used as surveillance. Banking, filing taxes, and other interactions with the government all generate documents that can be used in analogous surveillance methods. These forms of exhaust are older and lack the ease of use that newer forms offer. Nonetheless they present powerful and impactful surveillance power.


Transit
Wireless
Model: 03
Conforms to ANSI/UL 60950-1
Certified to CAN/CSA C22.2 No.60950-1
Conforms to ANSI/UL 60950-22
Certified to CAN/CSA C22.2 No. 60950-22
WESTELL, INC model :A99-TW1XAP7161-S
LISTED
US
Intertek
70379

Event Attribute | Local Attribute

Add Attribute

ID	Name	Value
1	Bald	No
2	Sunglasses	No
3	Eyeglasses	No
4	Hat	No
5	Moustache	No
6	Beard	No
7	Skin Tone	Light
8	Gender	Female
9	Age	Adult (26-35)
10	Head Color	Brown
11	Torso Pattern	Solid
12	Torso Color	White

Section 3: Backend

Face, both eyes, and mouth (frontal)

Face and both eyes, no mouth (frontal, looking down)

Face, single eye and mouth (profile)

$Class = Car$

$\overline{Speed} = {}^{100px}/_{sec}$ (42

$\overline{Size} = 971px^2$ (79"x5

$Duration = 3.1\ sec$

$Color = Yellow$

Face and single eye (profile, looking down)

Face Only (turned away or features not distinguishable)

© 2012 IBM Cor
All Rights R

These technologies and cameras are interesting, but the outputs would be of limited use if they just displayed on a screen in some room like old school CCTV cameras. What the cameras are plugged into often matters far more than the technical specifications of the camera itself. This is the power of big data, not in the massive troves of data themselves, but in the analytics they make possible. In New York City, there are two massive tech giants behind the analytic systems that feed off the surveillance infrastructure.

This system was developed in partnership between the NYPD & Microsoft. This is the "Domain Awareness System", announced in 2012 as part of the Lower Manhattan Security Initiative and continuing to this day. It is marketed as a "crime prevention and counterterrorism technology", and due to the closeness of the partnership, the NYPD gets a kickback every time Microsoft sells usage rights of the system to a new town or city. The NYPD carries out this massive data harvesting, a harvest that they directly profit from, without any warrants. They also use this data to feed an algorithm called "Patternizr", which attempts to predict crimes and criminals before they happen. These systems are, unsurprisingly, rife with racial bias. The constitutionality of the program is certainly questionable, but the ethical implications are clearer.

Some of the tracking capabilities of the DAS suite were developed by IBM. What is known about these features comes from years-old leaked documents and public releases, so it is likely that the software has grown more powerful than we now know. The software has identification and tracking capabilities for people and vehicles, indoors & out, with specialized algorithms for nearfield and midfield. The system identifies clothing, hair color, skin tone, gender, age, and other possibly identifying information of those caught in its gaze. All this data is stored in .xml files, ready to be used by the algorithm or police.

The police use these systems to identify protesters, often going on to brutalize them. The AI systems allow for easy filtering by race, providing further avenues for discrimination. The systems were trained, with questionable legality, using photos of minors, some as young as 11. This practice, along with the questionable morality, may actually make the software less effective

poration.
eserved.

in the long run. The algorithm learns to identify faces, but it is not equipped to understand how faces change as one grows into an adult. Not only does this make the training next-to-useless in identifying those in its system later, but it increases the risk of false positives for other children. This is not the only issue with the dataset fed to the algorithms in the NYPD's care. In a report titled Garbage in, Garbage out, Georgetown Law researcher Clare Garvie found significant problems with the rearing of the "AI", in ways that would lead to false identifications. In a review of all the NYPD surveillance tech, a report from the Brennan Center for Justice found not only myriad examples of free-speech-chilling activities, but numerous instances of widespread practices that would lead to similar false positives in identification and in arrest.

In 2017 the city council passed Local Law 49 for year 2018, which established a task force to investigate the use of these algorithms. This task force fractured in 2019, struggling to access data from the city and even finalize a working taxonomy. The report eventually produced by the task force read like a 36 page apology for not having more concrete information or recommendations. The task force was, in the words of Albert Cahn (executive director of STOP and fellow at Engelberg Center), a "spectacular failure"

In the wake of the protests over the summer of 2020, some companies offered symbolic gestures and semi-symbolic gestures of support. Amazon temporarily suspended sales of their facial recognition software "Rekognition" to police agencies. However a few months after, the company set up a massive deal with ICE for cloud computing. There was also an article in the Washington Post touting the announcement by Microsoft that it was following Amazon's example. The article left out any mention of Microsoft's DAS, which continues to be sold to police in the US and abroad, and includes facial recognition software. Microsoft also continues providing specialized cloud services to police through their Azure Cloud program.

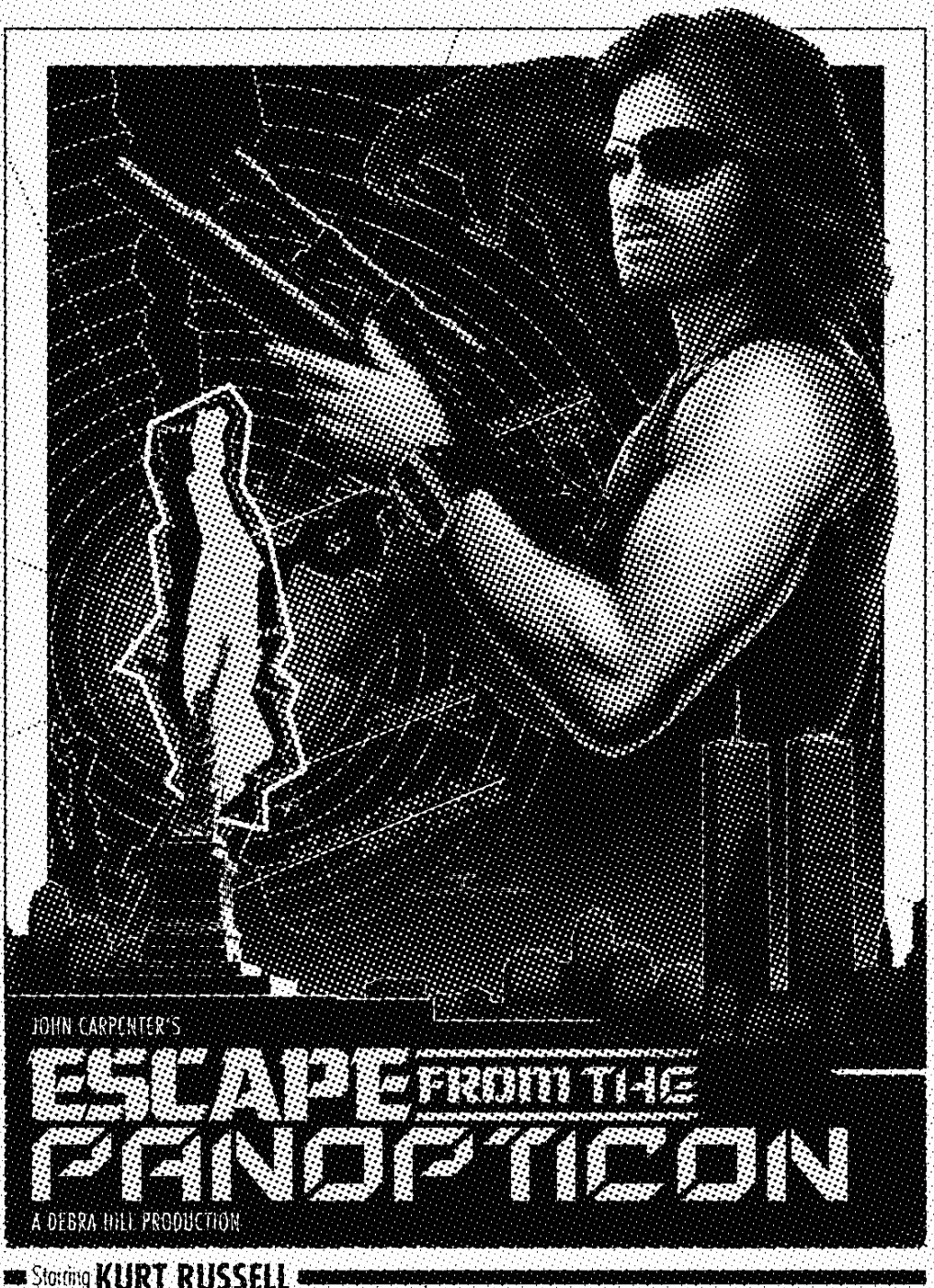
"I already am eating from the trashcan all the time. The name of this trashcan is ideology."

Slavoj Žižek,
The Pervert's Guide to Ideology

On Ideology and Stories

This text does not claim or attempt neutrality or objectivity, as such concepts are farcical and often merely serve as a shield for journalists from substantial critique on ideological grounds. Journalism should always be factual, but which facts to convey and in what way radically shifts the readers interpretation of the events. This is evidenced by the occasional factually coherent article on Fox News, when compared to similar articles in the New York Times or Al Jazeera, or Grayzone for that matter. Information has to be structured in some way as to give it a narrative, and it is in this narrative construction that we find ideology lurking.

Ideology subsumes discourse in subtle but altogether complete ways. Importantly here, it manifests itself in the structure in which we tell stories. Telling stories through the lens of individuals is a choice, one that is consistent with the individualism inherent to liberalism. This individualism says that the lens in which we should view the world is that of the individual. Liberal media touts the innovators, inventors, individual heroes with inspiring stories. The liberal justice system is similarly situated, finding and punishing the bad individuals. This kind of worldview is reinforced by the focus on individual stories, and by uncritically propagating it, journalists unintentionally mystify systems. This text, in an effort to counter neoliberal hegemony, will instead try to focus on the systems at play, rather than the individuals who occupy various positions of power within or those disempowered without these systems.


JOHN CARPENTER'S
ESCAPE FROM THE
PANOPTICON
A DEBRA HILL PRODUCTION
Starring KURT RUSSELL

In 1787 philosopher Jeremy Bentham outlined the design philosophy of the panopticon, a then-revolutionary prison design. The panopticon was a circular building with a central tower that could easily see every cell. This watching only went one way, and the central tower was supposed to be opaque from the cells, thus the prisoners would have no way of knowing if and when they were being watched. The idea was that because they knew they always could be watched, the prisoners would conform to rules set by the operators of the panopticon. This idea was drawn upon by postmodern philosopher Michel Foucault in his work Discipline and Punish: The Birth of the Prison. Foucault's work illustrates that, in short, the act of surveilling puts one in a position of power over those surveilled.

There are substantial philosophical critiques of Foucault's theory though. There is the substantial critique that prisons are set up very much like a panopticon, with arrays of cameras watching every cell and hallway. This surveillance has not created docile prisoners, with strikes, revolts, and interpersonal violence abounding in American prisons. Another aspect is that Foucault's theory rests on an underlying distinction between sites of surveillance (inside the panopticon) and those sites not surveilled (outside the prison). There is also the issue of temporality, where the panopticon only allows for the viewer to observe what is currently happening, modern technology unmoors surveillance in time and space. If the NSA, for example, takes an interest in you, they don't just know where you are as you read this, but almost everywhere you have been in the past, and are likely to go in the future. This is explored in more detail in Tobias Champion's essay Are We Living in a Post-Panoptic Society?.

Escape from these panoptic and post panoptic arrays of surveillance inspires various cyberpunk fantasies. Cory Doctorow's 2008 novel Little Brother includes an array of open source, hacked together subversions of government surveillance. Likewise, the conclusion of Bruce Schneier's Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World covered ways to subvert and confuse these surveillance systems.

Neither of these fantasies are really applicable to everyday life. They often require confusing or burdensome workarounds or the outright rejection of some technology. The problem is, of course, that escape is impossible. Surveillance is built into the technology we use in such a fundamental way that it is impossible to go back. Privacy can be worked into the design of new technologies, but the technology we have is built in such a way that meaningful privacy would require an unfeasible amount of reworking and rebuilding of infrastructure. What we are left with is the problem that the entity wielding the power of this surveillance is, to put it bluntly, fucking awful.

The covid-19 pandemic offers a helpful prism through which to view state action and the protection or safety offered to residents by the state in which they reside. How states reacted to the pandemic illustrates who and what is prioritized by the state. Crises create the possibility for change, and just as 9-11 opened the door for the patriot act, this pandemic has opened doors for new systems of surveillance.

As the pandemic started, China rolled out a system to track and contact trace. These systems seem not to actually utilize China's massive surveillance apparatus, opting for the technically simpler and more reliable options. According to UK-based law firm Norton Rose Fulbright, a name, ID card number (Resident Identity Card) and facial scan are required to sign up with either of the major tracking apps. The tracker can be downloaded as a standalone app, but the most popular are the tracking modules integrated in popular apps Alipay and WeChat. That report stated the Ministry of Information Industry Technology's data analysis platform primarily draws from cell phone data from the country's major telecom companies (China Mobile, China Unicom and China Telecom.) These apps display a QR code ranging from green to red, showing the user's likelihood of having covid based on who they have been in contact with. In early march of 2020 there was a major leak of data from the Alipay based app, releasing some users' names, addresses, and daily movements publicly. Sense then the apps have seemed to protect user's privacy better, at least from the public. These apps,

along with swift shutdowns and government assistance helped China bounce back successfully.

A similar project was started in the US: a joint venture from Apple and Google. This project was not an app, but merely an API (Application Programming Interface) to be used by other app developers at the state level. The tech behind the API was interesting, and shows a different design methodology at work when compared to the Chinese example. Rather than using the readily available data for the platform, the US venture opted to use a more novel approach. This was to use the BLE (Bluetooth low energy) module within phones to exchange info with other nearby phones, through a client-side encryption system that allowed notice of contact when a user received a positive test coupled with privacy and anonymity. Significantly, the tech was opt-in, meaning that users would have to go out of their way to sign up and download an interface to use the app, and the app would only be effective if most people used it. Adoption of the api and the apps that used it were inconsistent enough to make them unhelpful in contact tracing. Politicization of the virus also hurt the adoption and effectiveness of the tracking apparatus. It's less clear whether or not these contact tracking apps (CTAs) would have been as effective as they were in China, as a key aspect of CTA effectiveness if testing capacity, and the US struggled with testing for months into the pandemic.

The US and China have comparable surveillance apparatuses, but the difference in how they were used in covid was striking. China mobilized to use part of their apparatus to contact trace and coupled with testing was able to combat the illness effectively. The US struggled with an incompetent federal response and an inconsistent uncoordinated scrambling among the states. In New York City, the NYPD apparently checked the feeds of cameras in an attempt to "enforce social distancing". It does not appear that the NYPD was using their AI-powered backend to analyze the video or coordinating with New York State's contact tracing team. Surveillance is powerful and can be used positively, actually doing so requires mobilizing resources. When looking at China and the US, one state mobilized resources to protect its Populus, the other

left them to die.

These surveillance networks are being used by the US, particularly in the identification and expulsion of undocumented immigrants. The resources expended to identify immigrants are enormous, and involve the sharing of information between multiple massive public and private sector data streams. One effect of this surveillance is to force immigrants into the "surveillance gap". "The surveillance gap is a term used to describe those living in a surveillance society who fall under or outside the bounds of most surveillance systems. Life within a surveillance gap often subjects one to more hardship, violence, and discrimination. Tax filings are a surveillance mechanism commonly used by the US, which forces immigrants into off-the-books employment without the same protections offered to the rest of the labor force. Sense contact with the legal system heightens the risk or perceived risk of removal, immigrants are less likely to utilize legal protections offered to them via the courts. A similar dynamic exists in the utilization of police and reporting of crime. How the surveillance system is used, coupled with its integration into almost all aspects of society, mean that the targets of state expulsion policies are excluded from the safety net that surrounds the rest of society.

In New York City, the surveillance apparatus was turned onto Muslim communities in the wake of 9-11. This surveillance involved the input of innocent Muslim's information into NYPD reports and databases, subjecting them to myriad complications, discriminations, and hardships. The profiling was massive, and involved far more than simply focusing the existing surveillance apparatus on specific populations. The NYPD infiltrated mosques, student groups, and other community groups in the same way they would infiltrate the mob. This program included a detailed cartographic profiling of Muslims in New York.

The machinery of surveillance is also used against those who the US state does not officially condemn in the way that it does Immigrants, but nonetheless works against. The NYPD's Technical Assistance Response Unit sent undercover agents to infiltrate Occupy and BLM protests over 400

times, according to documents acquired via a FOIL lawsuit. The surveillance was extensive, providing real-time information tracking the flow of protests to police. What that real-time tracking means to those on the ground is clear if one has attended a large protest in New York. As the old police saying goes, you can't outrun the radio, the police set up roadblocks and choke points to disperse or brutalize protesters. The NYPD used their powerful facial recognition and tracking capabilities to identify and prosecute activist Derrick Ingram. The NYPD laid siege to the activist's apartment, using dozens of cops and dogs, for the alleged crime of yelling at a protest. They were able to do most of this in the open, as the restrictions on use of surveillance powers by police are virtually nonexistent. New technologies introduced into urban environments are quickly utilized by police to enhance their power. In San Diego, "smart streetlights" were installed in order to better manage traffic flows, once installed the traffic data sharing was cut off, and the streetlight cameras were exclusively used to identify and prosecute protesters.

The problem, it seems, is less in the essential existence of surveillance technologies. Many of these technologies provide significant benefits to users, conversely many useful technologies unavoidably subject users to some level of surveillance. The problem presents itself in how these technologies are utilized by those in power. In China, surveillance powers were used to contact trace and boost the fight against covid. In the US, these same powers were used to crack down against protest and persecute immigrants, all while leaving the Populus in danger from covid. Surveillance reinforces power, but the power that it reinforces can be welded to protect people, or to crush them.

A ZINE

BY

QUINN KOWITT