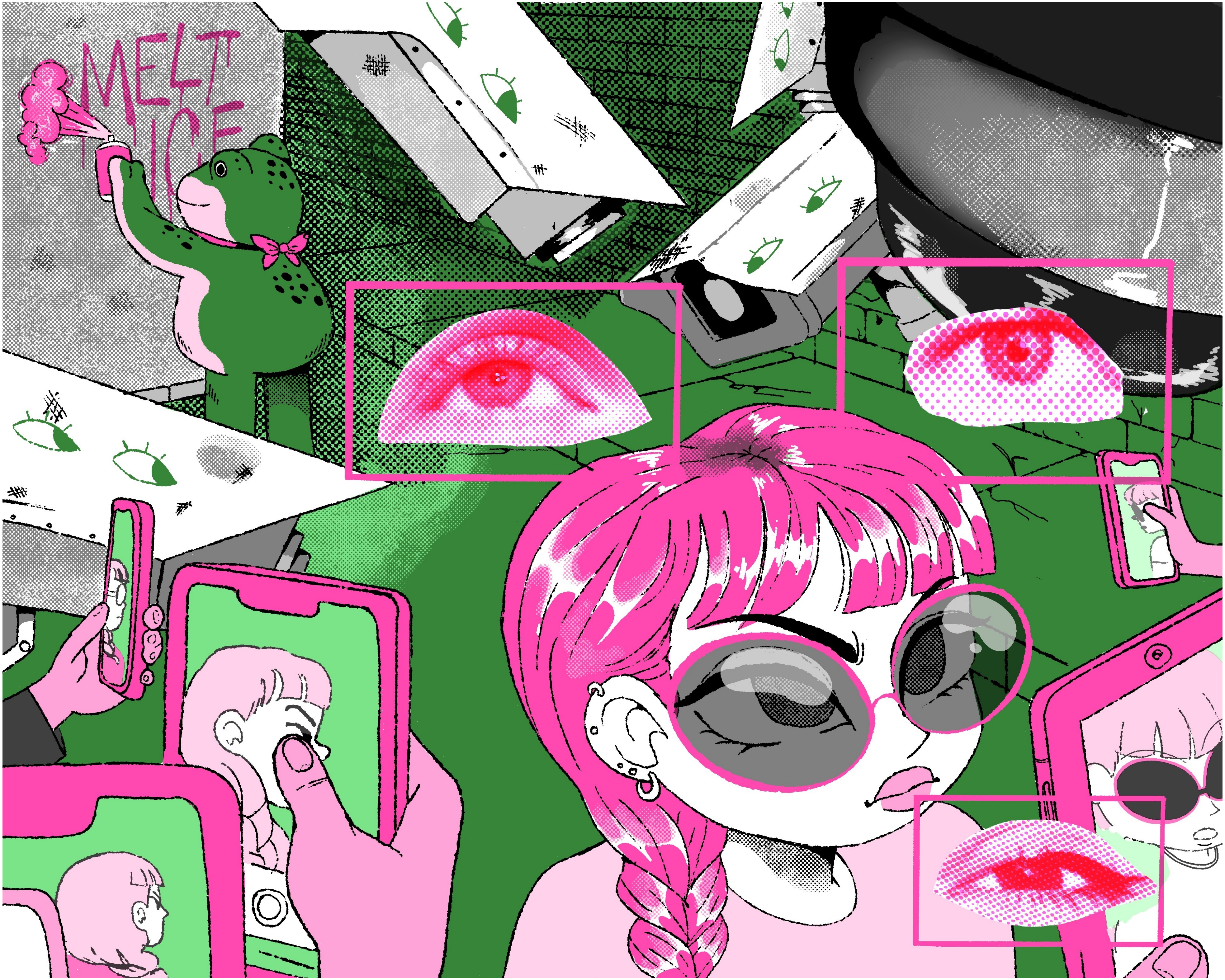

MELT
ICE

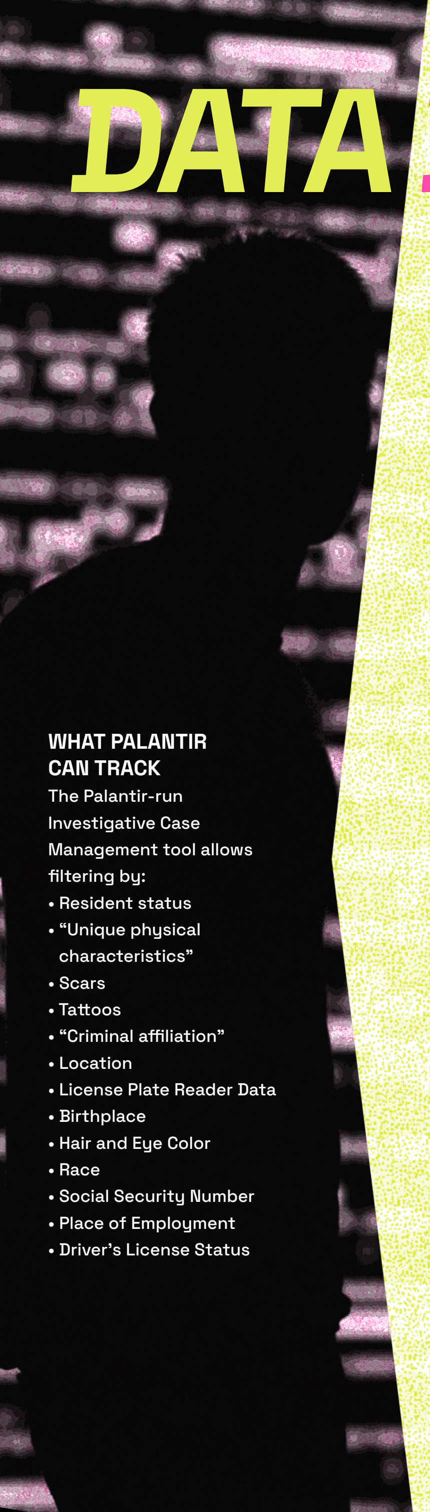
404 MEDIA

You are holding a zine about the surveillance tools used by ICE, and what we have learned so far about how you can resist this technology. This zine was reported and written by 404 Media, a journalist-owned investigative website and now, we suppose, a print publication. Our status as a small outfit of reporters who own the means of production (a website), means that we have the freedom to report on the topics we believe are the most important. For the last year, that has been Donald Trump's mass deportation campaign, and the technology powering it. The reporting comes from a mix of public records obtained from government procurement databases, court proceedings, Freedom of Information Act requests, interviews with activists, protesters, lawyers, and civil liberties experts, and information leaked to us by confidential sources within technology companies and government agencies. We feel confident in our reporting. What we feel less confident about is predicting where things go from here or giving advice about how you can protest or resist safely. Nothing in this zine should be considered advice on that front; ICE has many billions of dollars in funding and has been creative in its cruelty against the people it has detained and arrested. Likewise, surveillance companies know about many anti-surveillance tactics and "data poisoning" efforts, and are constantly working to render them moot by improving their technologies. And as journalists, our job is to find out what is happening, verify it, and publish it. So this zine is not full of advice, but it is full of information.

READ MORE

- You can find digital versions of these articles and of this zine at **404media.co/icezine**.
- Puedes encontrar una versión en español de este zine en **404media.co/icezine**.

We did not originally set out to spend most of the last year reporting on ICE. But we have watched the agency grow from an already horrifying organization into a deportation force that is better funded than most militaries. We have seen full-scale occupations of Los Angeles and Chicago, daily raids playing out in cities, towns, and workplaces across the country, and people getting abducted while they are at home or work, while they are shopping, or while walking down the street. As this has played out, we have focused on highlighting the ways that the Trump administration has used the considerable power of the federal government and the vast amounts of information it has to empower ICE's surveillance machine. Technologies and databases created during earlier administrations for one governmental purpose (collecting taxes, for example) have been repurposed as huge caches of data now used to track and detain undocumented immigrants. Privacy protections and data sharing walls between federal agencies have been knocked down. Technologies that were designed for local law enforcement or were created to make rich people feel safer, like license plate tracking cameras, have grown into huge surveillance dragnets that can be accessed by ICE. Surveillance tools that have always been concerning—phone hacking malware, social media surveillance software, facial recognition algorithms, and AI-powered smart glasses—are being used against some of society's most vulnerable people. There is not a ton of reason for optimism, but in the face of an oppressive force, people are fighting back, and we have tried to highlight their work in the zine, too.



DATA DANGERS

Palantir's ImmigrationOS shows why we need to resist mass data collection as often as possible.

BY JASON KOEBLER

Privacy advocates will say one of their core goals is to ensure that information collected for one reason is not used for another. Politicians have spent the last few decades encouraging undocumented immigrants to pay taxes, send their children to school, and otherwise interact with civilian parts of the government not associated with law enforcement. The promise made to them was that these interactions would be siloed, with walls preventing ICE from accessing them. The Trump administration has utterly destroyed these walls and protections. It started with a tool called Investigative Case Management, a Palantir database commissioned by the Obama administration, which connected different government databases and allowed for filtering across hundreds of different categories. Obama's own privacy impact assessment suggested this tool could be abused by future administrations and their shifting priorities.

That has now come to pass. The Trump administration tasked Palantir with building a more powerful tool, called "ImmigrationOS," a surveillance system intended to track people's movements, including so-called "self-deportations." Trump signed an executive order allowing the sharing of data between ordinarily separate agencies. That includes the IRS, which has agreed to provide immigrant addresses to ICE. The IRS is also using Palantir. This is why overbearing surveillance and data collection needs to be resisted early, and why privacy protections that have the force of law are so important: We are learning that privacy promises and policy positions can easily be changed. And "safeguards" and "guardrails" on surveillance technologies don't actually mean anything, and will be discarded to align with the administration in charge.

WHAT PALANTIR CAN TRACK

The Palantir-run Investigative Case Management tool allows filtering by:

- Resident status
- "Unique physical characteristics"
- Scars
- Tattoos
- "Criminal affiliation"
- Location
- License Plate Reader Data
- Birthplace
- Hair and Eye Color
- Race
- Social Security Number
- Place of Employment
- Driver's License Status

CHRIS YANG/UNSPLASH

META DEBATE

Should it be legal for ICE agents to wear smart glasses during raids?

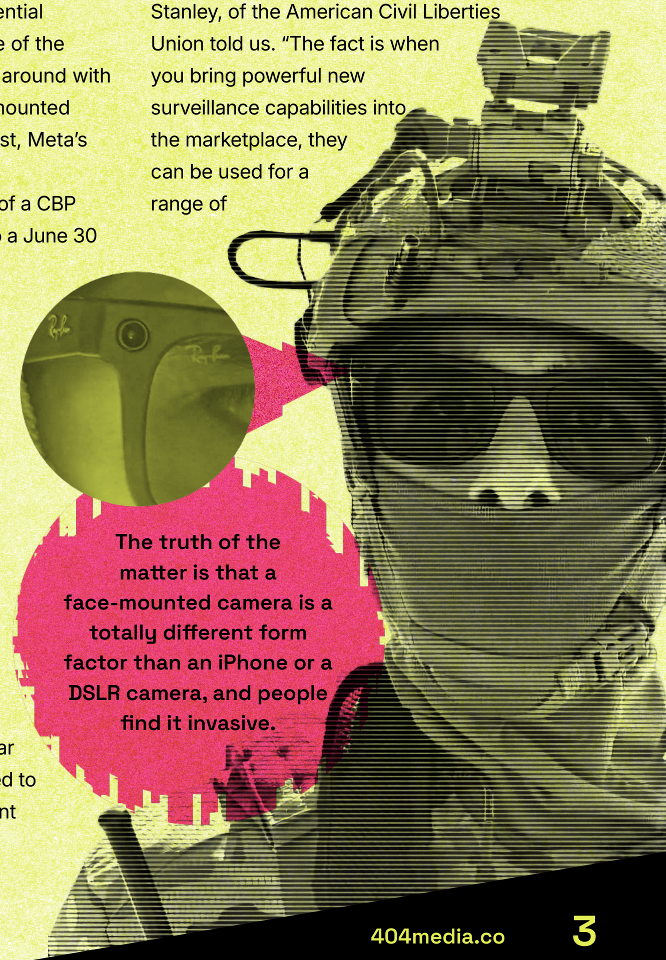
BY JASON KOEBLER

Government social media accounts have been filled with unhinged, highly stylized propaganda videos of ICE raids featuring agents chasing people down in Home Depot parking lots, crowded downtown areas, and residential neighborhoods, set to music. In some of the footage, you can see agents running around with DSLR cameras on stabilizers, body-mounted cameras, and, as we learned in August, Meta's Ray-Ban AI smart glasses.

404 Media got footage and photos of a CBP agent wearing Meta's smart glasses to a June 30 raid at a Home Depot in Cypress Park, Los Angeles. Two more agents were seen wearing the glasses at MacArthur Park in LA a week later. Meta's AI smart glasses feature a camera, live-streaming capabilities, integration with Meta's AI assistant, three microphones, and image and scene recognition capabilities. It's not clear why agents have been wearing smart glasses, and who actually owned them. CBP told us these were agents' own personal glasses and weren't issued by the department. But that raises questions about whether it's legal for the agents to wear them at all (CBP agents are not allowed to bring personal cameras to enforcement actions).

On billboards, Meta promotes its glasses as stylish accessories for influencers. But their use by CBP shows the state sees potential for them either as a surveillance device or as a tool to film propaganda videos. Meta says its tech should be treated like iPhones or any other cameras, and that it's unfair to point out that CBP agents are using them. But the truth of the matter is that a face-mounted camera is a totally different form factor than an iPhone or a DSLR camera, and people find it invasive. Meta has cozied up to the military in recent months, with Mark Zuckerberg announcing a new augmented reality and AI partnership with the defense contractor Anduril. Anduril's founder Palmer Luckey said his hope for the partnership was to "turn warfighters into technomancers."

"I think it should be seen in the context of an agency that is really encouraging its agents to actively intimidate and terrorize people," Jay Stanley, of the American Civil Liberties Union told us. "The fact is when you bring powerful new surveillance capabilities into the marketplace, they can be used for a range of



The truth of the matter is that a face-mounted camera is a totally different form factor than an iPhone or a DSLR camera, and people find it invasive.

FLOCKOFF

BY JASON KOEBLER

In 2018, a brand new surveillance startup began marketing its solar powered, license plate-reading cameras to homeowners associations around the country. The company, Flock Safety, allowed homeowners associations to see who was coming in and out of their neighborhoods, and could even detect when a "nonresident" car drove by. The company called this a "virtual neighborhood gate that keeps communities safe," and issued a press release when the technology was used to find a bike thief: "the Flock camera system along my street captured the criminal's face, tag number, and car in enough detail to view my bike in the trunk and provide local law enforcement enough evidence to arrest the criminal," the victim said in a case study widely shared by the company.

> Flock's spread throughout the United States and its mission creep has shown the danger of networked surveillance technologies.

At the time, Flock was being marketed mostly to expensive neighborhoods. The pitch, at least initially, was for homeowners associations to pass information on property crimes to police.

Fast forward to 2025, and Flock's automated license plate reader cameras (ALPRs) have become one of the most pervasive types of physical surveillance in the country. It has grown from a concerning but basically discrete piece of technology designed to surveil a single road or neighborhood to a network of roughly 6,000 different cities, police departments, and other entities across more than 80,000 cameras nationwide. Flock also sells to malls, hardware stores such as Home Depot and Lowes, hospitals, schools, and churches; it also sells controversial and highly contested "gunshot detection" microphones and drones that fly themselves and autonomously respond to emergency calls. Whenever a car drives past a Flock camera, several photos are taken and that information is logged into the company's database, with the time and location of that vehicle, allowing police to create detailed records of a specific person's movements.

Last year, using public records requests, we were able to obtain several Flock "network audits," which are huge spreadsheets of information about what police are using the Flock network for, included in a "reason" tab that cops fill out when performing a search. It turns out, cops are using it for essentially everything. A two-week period of data had more than 160,000 nationwide lookups with reasons that ranged from "theft" to "hit and run" to specific case numbers and things as broad as "investigation," "crime," or "wanted." Many of the entries don't have any reason listed at all.

But what was most striking was our finding that local police were performing thousands of searches for "immigration," "ICE+ERO," "illegal immigration," and "HSI," which stands for Homeland Security Investigations, a division of ICE that performs, among other things, workplace raids. This was particularly notable both because it showed Flock was being used for immigration enforcement, but also because at the time, neither ICE nor DHS had any contract with Flock; essentially, local police were giving the Trump administration a backdoor way to look for undocumented immigrants by performing lookups at the behest of ICE. In some cases local police were working under a program called 287(g), an ICE program that allows local police to do immigration enforcement. Our investigation also found that local police were often searching Flock cameras in states where it was illegal for them to do so. Police in Texas would search not just their own cameras, but also cameras in California and Illinois, where state law prohibits local police from doing immigration enforcement.

Our reporting has shown that DHS and ICE not only have great interest in mining license plate data for immigration enforcement, they are accumulating many different ways of collecting that data. ICE has contracts with Motorola, which also makes ALPR cameras, and uses a smartphone app called Mobile Companion to search license plates. It can then marry that information with data from the data broker Thomson Reuters. Motorola also advertises facial recognition capabilities and the supposed ability to predict the "future locations" of vehicles to ICE. In short, ALPRs have become one of the most widely used types of surveillance technology on the market, and it is now incredibly difficult to drive anywhere in the country without your locations being logged. This technology is now explicitly being used directly against undocumented immigrants.

Soon after our discovery, Illinois cracked down on Flock, and Flock added several safeguards to theoretically prevent some of this overreach. But the company then began what it called a pilot program directly with the Department of Homeland Security. Flock's spread throughout the United States and its mission creep has shown the danger of networked surveillance technologies, and also shows how quickly and easily surveillance companies can leverage the false promise of "preventing crime" into thousands of contracts with towns and cities throughout the country, one city council at a time. It also shows how surveillance tools marketed and sold to the rich are inevitably used against society's most vulnerable people. The silver lining, if there is one here, is that a handful of cities have ended their Flock contracts, citing our reporting on its use in immigration cases and a separate case in which it was used against a woman who had a self-administered abortion in Texas.

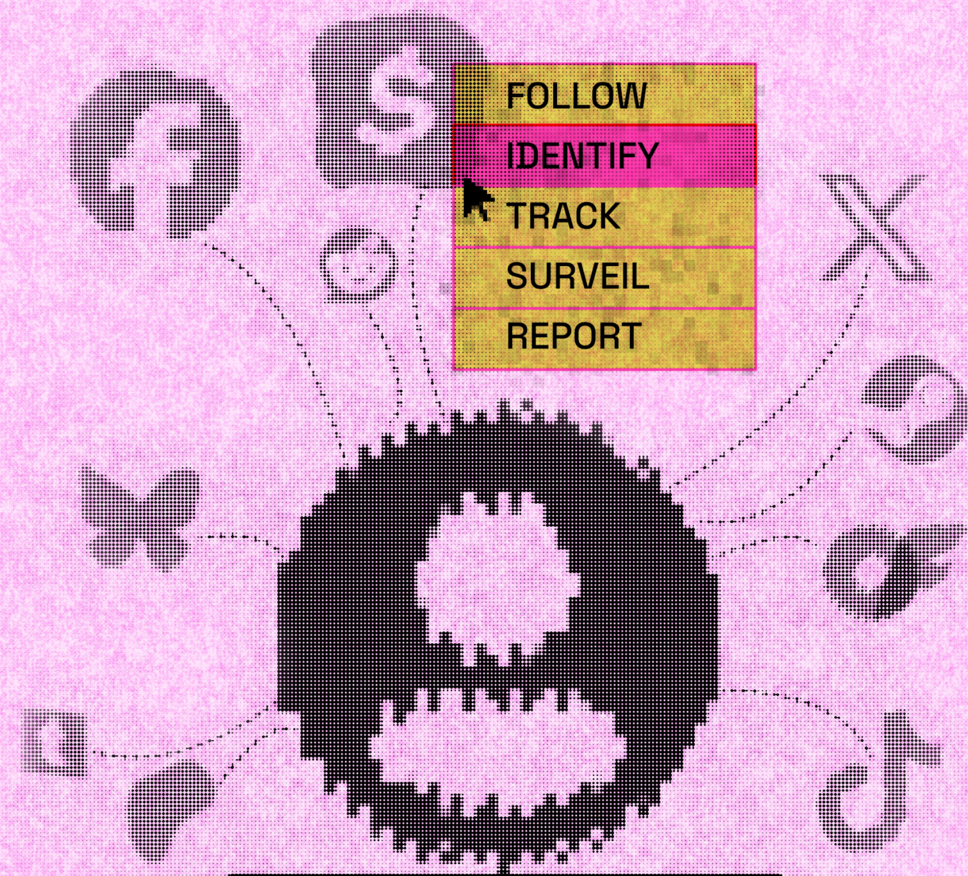
BY THE NUMBERS

6,000
U.S. cities connected to the Flock network

80K+
Flock cameras nationwide

160K
Flock Network police lookups in a single recent week

HANDOUT PHOTO/FLOCK



THE SHADOW FOLLOWING YOU ONLINE

BY JOSEPH COX

ShadowDragon is a social media surveillance company which sells its tech to ICE. The company has the ability to monitor public activity on all sorts of social networks, apps, and websites. From Bluesky to Onlyfans to CashApp to Meta platforms, we obtained a list of more than 200 sites ShadowDragon is keeping tabs on.

FONT AWESOME/ERNIE SMITH ILLUSTRATION

ICE's Silent Exploit

ICE bought the most powerful phone hacking tool you've never heard of. We're suing to learn why.

BY JOSEPH COX

Paragon, an Israeli company, sells hacking tools to let government agencies remotely break into mobile phones without the target even clicking a link. And ICE has paid this company $2 million.

How it works: Paragon's software, called Graphite, uses a variety of exploits to break into a target's phone. One of those involves sending a PDF to a target over WhatsApp. The phone loads the PDF, which contains the exploit, and the phone is silently hacked.

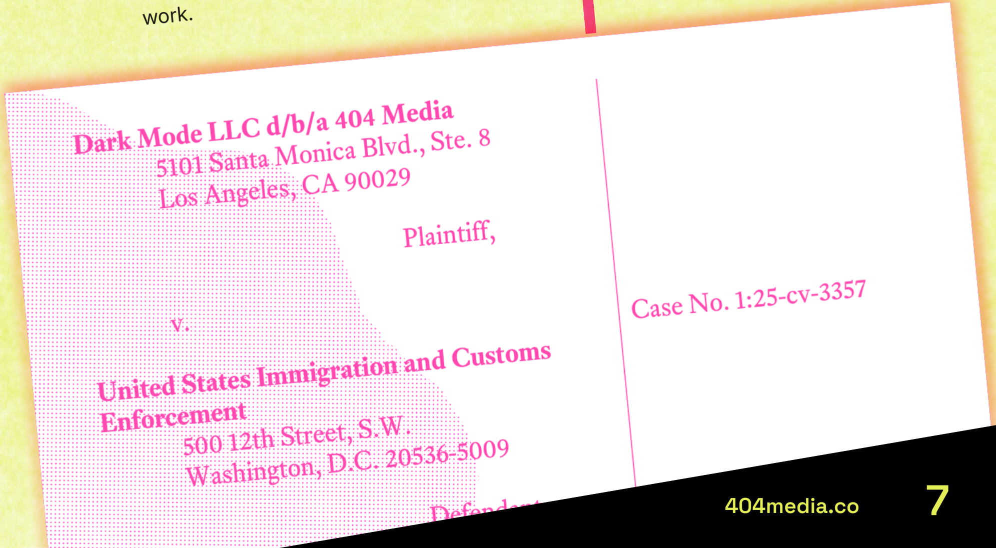
The data it can get: Paragon is focused on obtaining the contents of messages from encrypted chat apps, like WhatsApp and Signal, or other communication tools like Facebook Messenger or Gmail.

How you can protect yourself: Keep your phone fully up to date, and if available, use a feature like Apple's Lockdown mode which makes it harder for this sort of malware to work.

WHY WE'RE SUING

ICE has refused to hand over basic contracting documents in response to our Freedom of Information Act (FOIA) request. So in September we filed a lawsuit against ICE demanding it release the records: "404 Media has asked ICE to disclose agency records relating to its contract with a company known for its powerful spyware tool whose potential use in the agency's ongoing mass-deportation campaign has prompted lawmakers, civil liberties organizations, and immigration groups to express deep concerns over potential civil rights abuses," our lawsuit says.

We want these documents because they may show why exactly ICE bought this technology and what it plans to do with it.



Dark Mode LLC d/b/a 404 Media
5101 Santa Monica Blvd., Ste. 8
Los Angeles, CA 90029

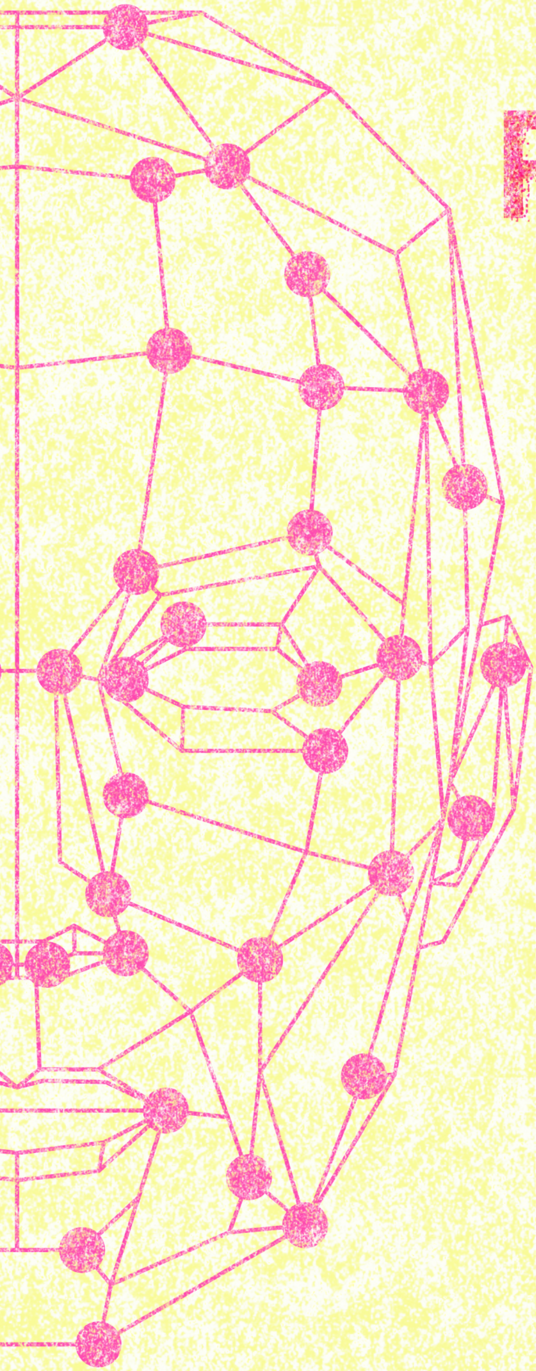
Plaintiff,

v.

United States Immigration and Customs Enforcement
500 12th Street, S.W.
Washington, D.C. 20536-5009

Defendant

Case No. 1:25-cv-3357



FREEPIK

FACES, PLEASE

Facial recognition was once seen as a bridge too far for surveillance tech. ICE's Mobile Fortify has changed the rules.

BY JOSEPH COX

"He's refusing to be ID'd," one officer from ICE's Enforcement and Removal Operations says to a colleague next to him. The group of federal officers are crowded around a car in a residential street, speaking to the driver through his rolled down window.

"I'm an American citizen," the driver of the car says.

"Listen. Listen. I'm being very polite, aren't I?" the ICE officer replies. I have to go to work, the driver replies. Where do you work, one of the officers asks. "Don't worry about it," the driver says.

"I'm an American citizen so leave me alone," he adds.

"Alright. We just have to verify that," one of the officials says.

The altercation continues. One of the officers says "look at me real quick." He then points his smartphone's camera at the driver's face.

"Hey, so listen," the officer continues. "If you could take your hat off, it'll be a lot quicker."

"I'm going to run your information."

The officer meant he was going to use facial recognition on the driver to verify his identity and immigration status.

This is the new reality in the U.S. Groups of officials from ICE and other agencies question people based on their skin color, accent, or how they look. When they decline to provide identification, law enforcement scans their face. ICE's facial recognition app, called Mobile Fortify, queries an unprecedented number of government databases, and tells the officer the person's name, date of birth, "alien number," and whether they've been given an order of deportation. ICE says people cannot refuse to be scanned by this tech, and believes the app's results provide a "definitive" determination of someone's status, even overriding a birth certificate.

Launching facial recognition products to identify strangers was considered such a dangerous technology that Meta and Google have thus far refused to release such tools. Amazon pitched its Rekognition product to ICE. But widespread access to this technology was popularized by a company called Clearview AI, which scraped billions of images from the web, and sold its face matching capability to local, state, and federal authorities alike. Clearview, mostly, was designed for criminal investigations. ICE's use of a facial recognition tool to unmask people in order to detain them for immigration violations was the natural next step.

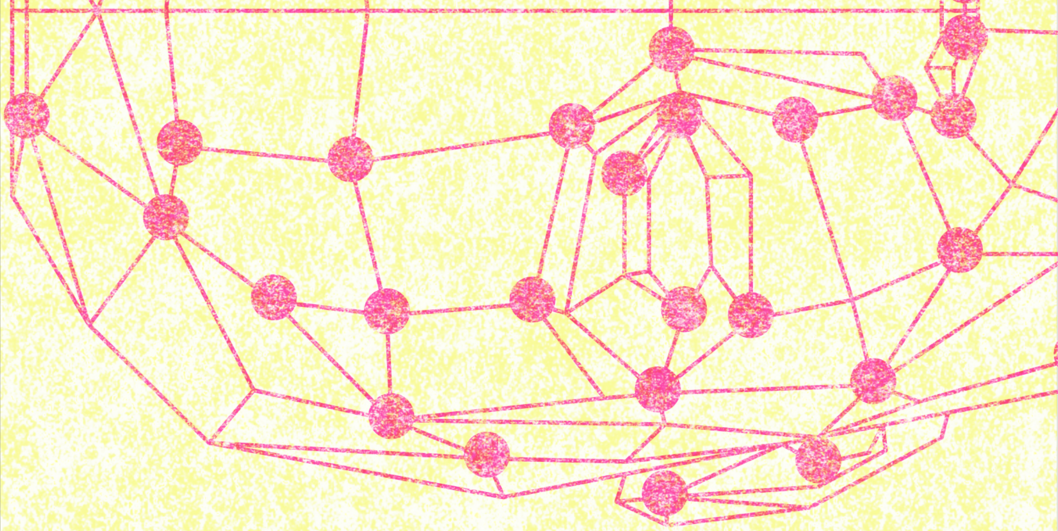
We received leaked ICE emails that revealed Mobile Fortify's existence. We then viewed user manuals for the tool. They showed the app runs a subject's face against a databank of 200 million images. Users can also perform a "Super Query," which searches the National Crime Information Center, an FBI-maintained database; another system which includes any outstanding state warrants against someone; and a number of CBP systems.

> Launching facial recognition products to identify strangers was considered such a dangerous technology that Meta and Google have thus far refused to release such tools.

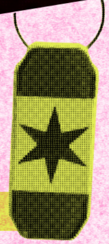
"The photograph shown [...] is the photograph that was taken during the individual's most recent encounter with CBP, however the matching will be against all pictures CBP may maintain on the individual," a document we obtained reads.

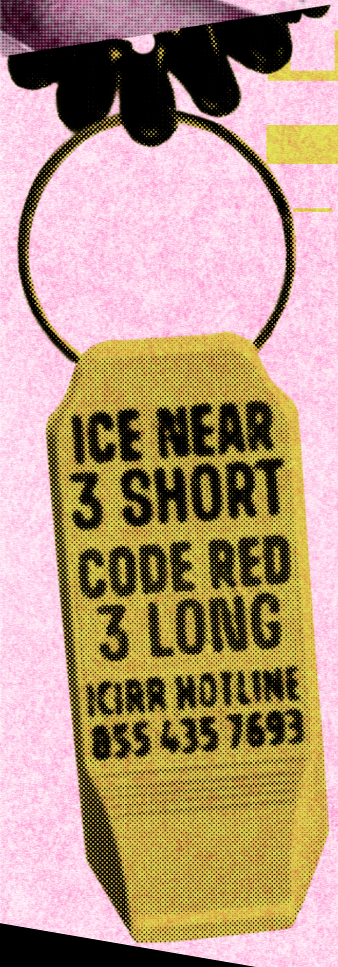
CBP then launched what appears to be a stripped-down version of Mobile Fortify for local cops, called Mobile Identify. With this, police scan a person's face, and it tells them whether to contact ICE about the subject or not, and provides a reference number.

For years, people warned that facial recognition tech would end up in a situation like this, where officers are able to identify essentially anyone on the street. Over the last year, that warning has proved prescient.



HANDOUT PHOTOS





WHISTLE BACK

How communities are 3D-printing whistles to fight back against ICE

BY JOSEPH COX

During the recent Operation Midway Blitz, multiple Chicagoans 3D-printed whistles to warn their community when ICE officials were in the neighborhood. Three short blows for "ICE is near," and three long blows for "Code Red."

People in Chicago made their own whistle designs and put them online for anyone to print. You can see an example here: **https://bit.ly/3MHoLlq**

3D printers work by taking a design and then building the item layer-by-layer. The 3D-printed whistles are cheaper than buying them on Amazon and subvert a supply chain that supports big tech, putting the means of production directly in the hands of the impacted community. Some of the whistles are printed with critical information or messages of solidarity on them, and whistles are a quick way of communicating across languages. The goal is to "prevent as many people from being kidnapped as possible," Aaron Tsui, who has been printing the whistles, told us.

HANDOUT PHOTO

FLIGHT RISKS

Hackers put a target on federal agents—and airlines helping with deportations.

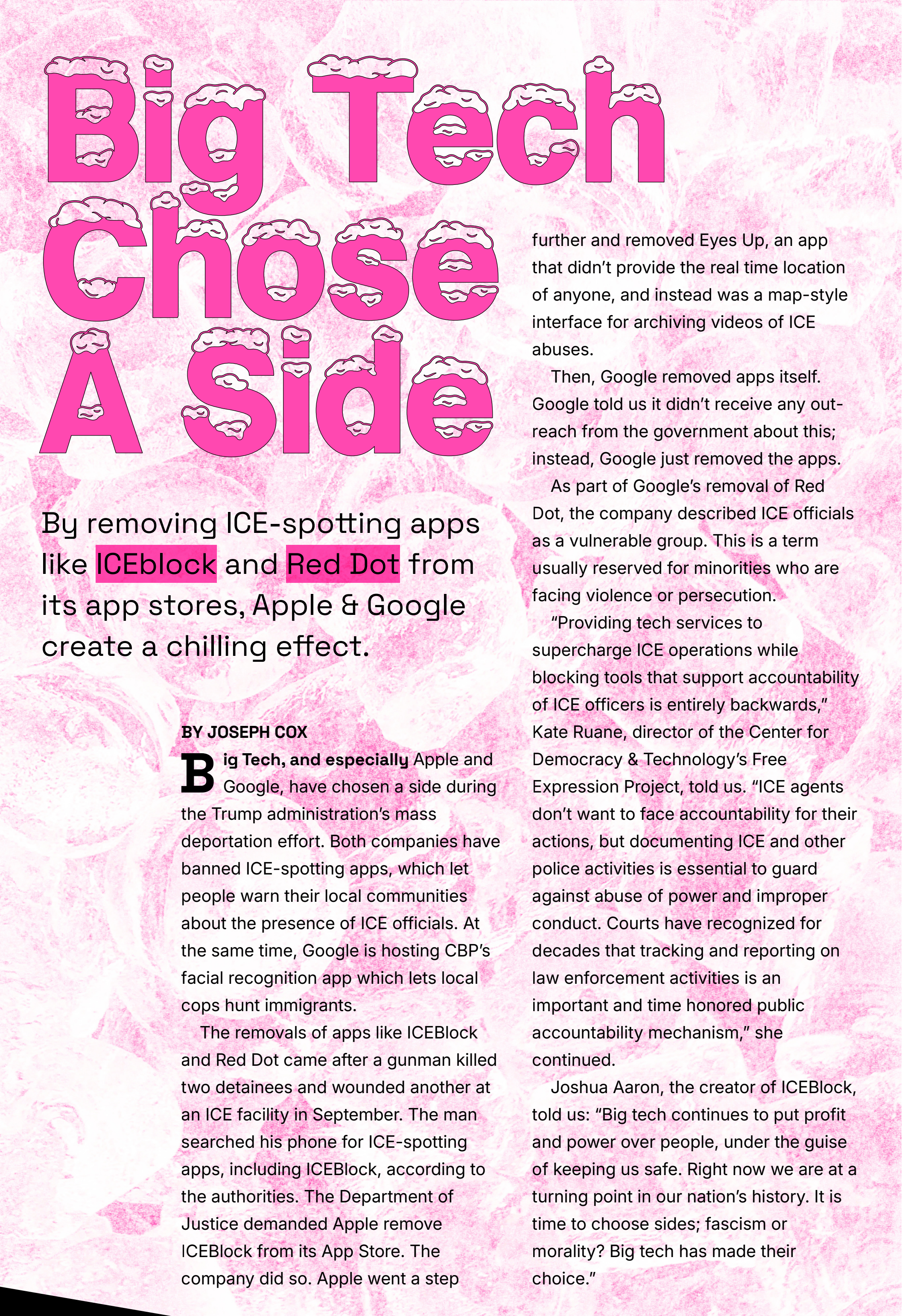
BY JASON KOEBLER

The cruelty of the Trump administration has, in a way, inspired hackers to fight back. Most notably, in October, a group called "Scattered LAPSUS$ Hunters" dumped spreadsheets containing the apparent identities of 680 DHS officials (including ICE agents), 170 FBI email addresses and their owners, and 190 Department of Justice Officials: "I want my MONEY MEXICO," someone associated with the group said at the time, referencing an unproven Trump administration claim that Mexican cartels had started offering monetary bounties for the doxing of ICE agents. The data came from a massive hack of Salesforce customers. 404 Media verified that at least some of the information was correct, and included government officials' names, addresses, phone numbers, and email addresses.

The event was the second major recent immigration-related hack. In May, GlobalX, a private airline that has been flying deportation flights for the administration, was hacked. Hundreds of flight manifests, which showed the names of people scheduled to be on specific flights, including crew members and people being deported, were leaked to 404 Media by someone claiming to be associated with Anonymous.

Most notably, we obtained manifests for three March 15 deportation flights from Texas to El Salvador, which became the subject of a Supreme Court case and intense public scrutiny because a judge tried to block the flights. Kilmar Abrego Garcia, a Maryland man, was illegally deported to the notorious CECOT megaprison on one of these flights. The hacked flight manifests revealed that a man who was "disappeared" by ICE was actually put on one of the flights to El Salvador, and also revealed dozens of additional passengers who had not appeared on any government lists at all whose whereabouts were entirely unknown to their families until they saw them on government propaganda videos or images released from CECOT. This included Keider Alexander Flores Navas, a Venezuelan man whose family eventually recognized him in a CECOT photo but whose name was not released by the U.S. government as having been deported.

"We have this list of people that the U.S. government has not formally acknowledged in any real way and we pretty much have no idea if they are in CECOT or someplace else," Michelle Brané, executive director of immigrants rights group Together and Free, told us about the hacked manifests.



JAN ANTONIN KOLAR/UNSPLASH

Big Tech Chose A Side

By removing ICE-spotting apps like ICEblock and Red Dot from its app stores, Apple & Google create a chilling effect.

BY JOSEPH COX

Big Tech, and especially Apple and Google, have chosen a side during the Trump administration's mass deportation effort. Both companies have banned ICE-spotting apps, which let people warn their local communities about the presence of ICE officials. At the same time, Google is hosting CBP's facial recognition app which lets local cops hunt immigrants.

The removals of apps like ICEBlock and Red Dot came after a gunman killed two detainees and wounded another at an ICE facility in September. The man searched his phone for ICE-spotting apps, including ICEBlock, according to the authorities. The Department of Justice demanded Apple remove ICEBlock from its App Store. The company did so. Apple went a step further and removed Eyes Up, an app that didn't provide the real time location of anyone, and instead was a map-style interface for archiving videos of ICE abuses.

Then, Google removed apps itself. Google told us it didn't receive any outreach from the government about this; instead, Google just removed the apps.

As part of Google's removal of Red Dot, the company described ICE officials as a vulnerable group. This is a term usually reserved for minorities who are facing violence or persecution.

"Providing tech services to supercharge ICE operations while blocking tools that support accountability of ICE officers is entirely backwards," Kate Ruane, director of the Center for Democracy & Technology's Free Expression Project, told us. "ICE agents don't want to face accountability for their actions, but documenting ICE and other police activities is essential to guard against abuse of power and improper conduct. Courts have recognized for decades that tracking and reporting on law enforcement activities is an important and time honored public accountability mechanism," she continued.

Joshua Aaron, the creator of ICEBlock, told us: "Big tech continues to put profit and power over people, under the guise of keeping us safe. Right now we are at a turning point in our nation's history. It is time to choose sides; fascism or morality? Big tech has made their choice."

PHOTO BY JASON KOEBLER

Why Frogs?

Yeah, it's nonsensical. But there's a certain logic to the viral protest gear.

BY MATTHEW GAULT

During a cruel presidency where many are in desperate need of hope, an inflatable frog stepped into the breach. The Portland Frog has become a surprisingly practical symbol of protest against ICE and Trump's mass deportation campaign. The absurd juxtaposition of an inflatable amphibian standing up to heavily armed and heavily armored ICE agents has hit particularly hard. But the frog is also a practical piece of passive resistance protest kit in an age of mass surveillance, police brutality, and masked federal agents disappearing people off the streets.

Symbols are important to movements, but the best protest symbols have a practical edge.

On October 2—just a few minutes shy of 11 PM in Portland, Oregon—a federal agent shot pepper spray into the vent hole of Seth Todd's inflatable frog costume. Todd was protesting ICE outside of Portland's U.S. Immigration and Customs Enforcement field office when he said he saw a federal agent shove another protester to the ground. He moved to help and the agent blasted the pepper spray into his vent hole.

Todd was unmoved. "I've definitely had spicier tamales," he told the Oregonian. The moment was shared and re-shared online and Todd's froggy form became more than just a protestor. He became a symbol.

Symbols are important to movements, but the best protest symbols have a practical edge. During anti-authoritarian protests in Hong Kong from 2014 to 2019, the people in the streets used yellow umbrellas to signal their solidarity. The umbrella doubled as a means of disrupting pepper spray and warding off small thrown objects. It's important to remember the human inside the frog or behind the umbrella. These inflatable costumes contain brave humans who are standing up to ICE agents terrorizing American cities.

Next to a frog, the self-seriousness of ICE agents and a military that has been turned into an occupying force against the nation's own people is shown for what it is: absurd. For people who've been pointing out how horrifying and absurd Trump is for a decade, there's something about the frog among the police that makes people see it. It's a meme that renders everything about our current political moment down into a single image, a hieroglyph that explains the first year of the second Trump presidency.

Fighting Surveillance in Style

The right outfits may (or may not) mess with ever-present cameras.

BY SAMANTHA COLE

The same algorithms that use your face to unlock your phone are being used by cops to recognize you in traffic stops and immigration raids. Surveillance companies coat the country with cameras, performing tens of billions of scans of vehicles a month and sell the data to police departments. But there are ways to disguise yourself from facial recognition systems in your everyday life that don't require owning clothes with a special design, or high-tech anti-surveillance gear.

↑ **CV Dazzle,** dating to 2010, attacked the problem with facepaint and hairstyles, but proved ineffective as camera tech improved.

→ **Adversarial Fashion,** launched in 2019, aims to pollute license plate reader data by outfitting the privacy conscious in fake plates.

One of technologist Adam Harvey's earliest forays into anti-surveillance design was CV Dazzle, which used strategically applied facepaint and hair to fool a specific facial recognition algorithm. But that was in 2010, and face paint is no longer useful for evading facial recognition. Since then, the anti-surveillance design genre has expanded to expensive streetwear and wearables. But most of the wearables in this genre are unreliable, with algorithms and camera resolution improving all the time. A lot of anti-surveillance fashion looks cool, but doesn't actually work.

Most facial recognition systems break down the elements of a face into its parts: the shape of your eyes, lips, nose, and even ears, and the distances between each part of your face, combined with skin color and numerous other factors. They boil your face down to a numerical value. If that value matches existing images a system has in its database closely enough, including other images of your face, it's verified as you.

Anti-surveillance fashion can still make a statement even if it doesn't work perfectly.

FACE-HIDING ACCESSORIES

Hats: A baseball cap or brimmed hat can be an effective way to make your facial features—especially your eyes—harder to scan.

Masks: A target at protests, but remain an excellent way to cover your face from cameras.

Big Sunglasses: Shades that cover as much of your features as possible.

Knowing this, you probably already own the most effective anti-surveillance fashion: a cloth mask.

"Despite how anybody may try to discourage you, covering your face with a face mask is still very effective," technologist and fashion designer Kate Rose told me. In 2019, Rose created Adversarial Fashion, a line of clothing that's covered in fake license plates, meant to pollute the data collected by automatic license plate readers.

Adding a few common items to your outfit can reduce the likelihood that biometric scanning systems can identify you accurately. Big sunglasses, covering your chin and mouth, and wearing a baseball cap or brimmed hat that obscures your features from cameras placed above can all bring that score down. And if you want to really step up your sunglasses game, you could get a pair of glasses that block infrared wavelengths from cameras.

The creator of infrared-blocking sunglasses line Reflectables, who asked to go by Skitch, told me he sees the anti-surveillance "fashion" market becoming more mainstream with companies like Zenni selling glasses that block some types of facial recognition. "I see the landscape of anti-surveillance wearables becoming popularized and monetized," Skitch said. "If people with money find out that an area of business exists without them making money, they will certainly find a way to gather that market, that money."

Anti-surveillance fashion can still make a statement even if it doesn't work perfectly. "People get a chance to talk to each other about what's important to them, and it actually helps people to understand something that's often kind of techy and abstract about how a piece of prevalent surveillance tech works," Rose said. If a license plate camera database can be foiled by a t-shirt, maybe we should think twice about putting a camera on every corner.

"I like the definition of privacy from the Cypherpunk Manifesto: 'Privacy is the power to selectively reveal yourself,'" Harvey said, referring to technologist and cryptographer Eric Hughes' 1993 call for encrypted information systems. "By allowing other people to collect, watch or monitor you... It's a power dynamic that puts you on the losing end. It's really about power and individual agency, but there's also a destructive political and democratic component to allowing these mass surveillance systems to grow even larger."

← **Reflectacles,** a line of privacy-centric eyewear, prevents infrared cameras from seeing your eyes.

HANDOUT PHOTOS

404 Media was founded by:
Jason Koebler
Samantha Cole
Emanuel Maiberg
Joseph Cox

Contributors:
Becky Ferreira
Matthew Gault
Evy Kwong

Layout by
Ernie Smith
Cover art by
Veri Alvarez

Risograph printing by
Punch Kiss Press in Los Angeles

Thank you to
heaven2nite, LA Fights Back! & CHIRLA

About Us

404 Media is a journalist-owned, journalist-operated independent media company that was founded in August 2023. We all used to work at VICE Media, a company that gave us an incredible amount of editorial freedom and experience, and also a front seat view into how to not run a company. We have spent the last two-and-a-half years trying to build something more sustainable and more human in a world and on an internet that feels more automated and more reckless than ever. We believe that it is possible for a small team of dedicated reporters to do impactful, groundbreaking accountability journalism on the companies and forces of power that are pushing us to a more inhumane world without overwhelmingly focusing on appeasing social media and search algorithms. And we believe it is possible to do that in a financially sustainable way.

One way we believe we can become less reliant on distribution models dominated by big tech companies is by making our work available in print, where it can be mailed, sold in stores, handed out at concerts. It can be read and passed to a friend, donated to a thrift store and discovered by someone killing time on a weekend, or tossed in a recycling bin and rescued by a random passerby. It is a piece of physical media that can be organically discovered in the real world. This zine is our first experiment at a print product, and, like everything else we do, we are starting very small in hopes that people like it, support it, and that we can do more of them in the future.

404 Media needs the support of paying subscribers. You can become a paying subscriber at 404media.co. If you would like to make a tax-deductible donation to support our work, please email **donate@404media.co.** Otherwise, you can reach us at **jason@404media.co** or **support@404media.co**.

Like other projects we have done, we have leaned on both our virtual community of friends, sources, and experts, and our local community to help us create this.