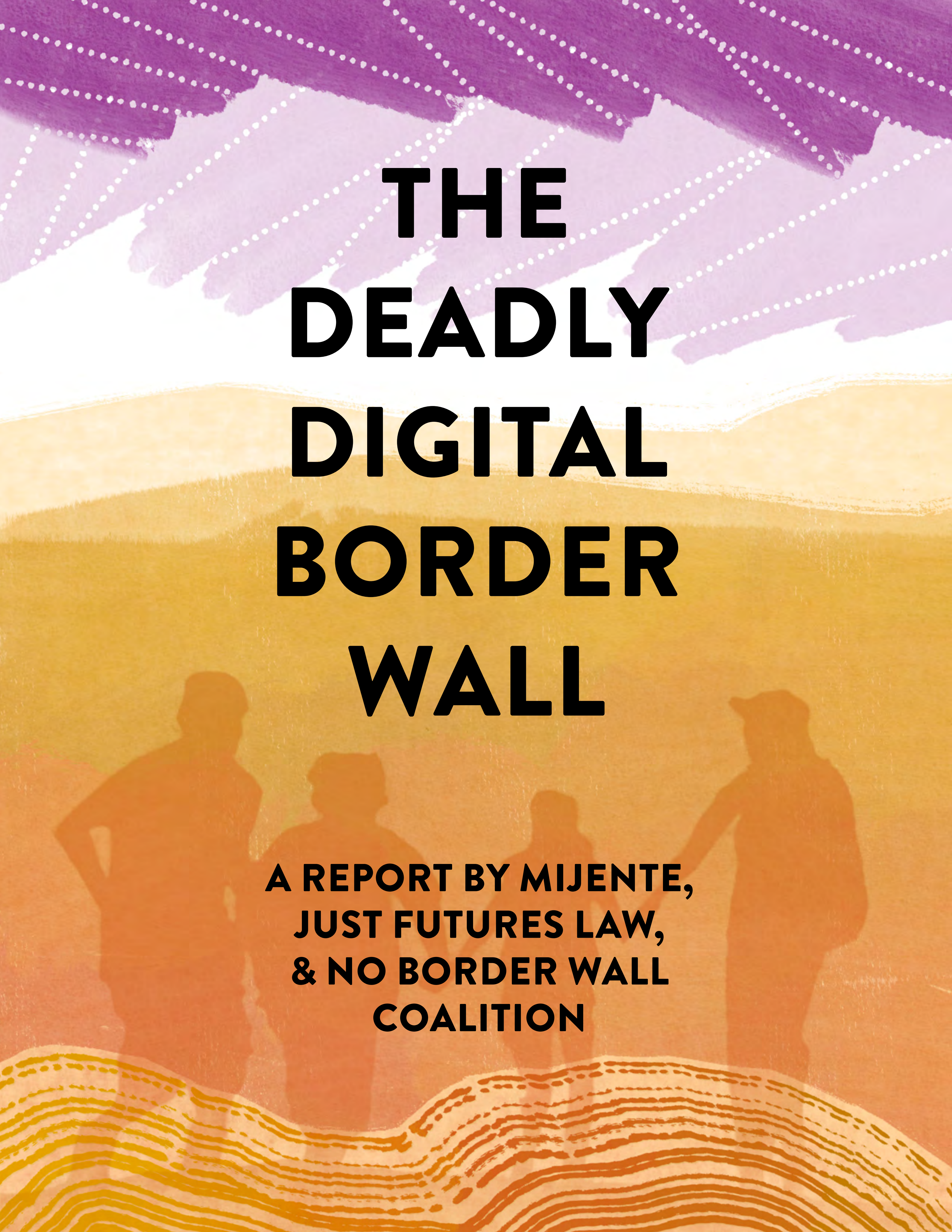


THE DEADLY DIGITAL BORDER WALL

A REPORT BY MIJENTE, JUST FUTURES LAW, & NO BORDER WALL COALITION

TABLE OF CONTENTS

This report was written in close partnership between Mijente, Just Futures Law, and the No Border Wall Coalition.

Mijente is a national organizing hub and political home for Latinx and Chicanx people that's pro-Black, pro-Indigenous, pro-worker, pro-woman, pro-lesbian, gay, bi, trans, and queer, and pro-migrant. It leads the #NoTechForICE campaign, organizing against the surveillance machinery supplied by Silicon Valley for immigration and border policing.

Just Futures Law is a transformative legal organization that defends and builds the power of immigrants' rights and criminal justice activists, organizers, and base-building community groups working to disrupt and dismantle our deportation and mass incarceration systems.

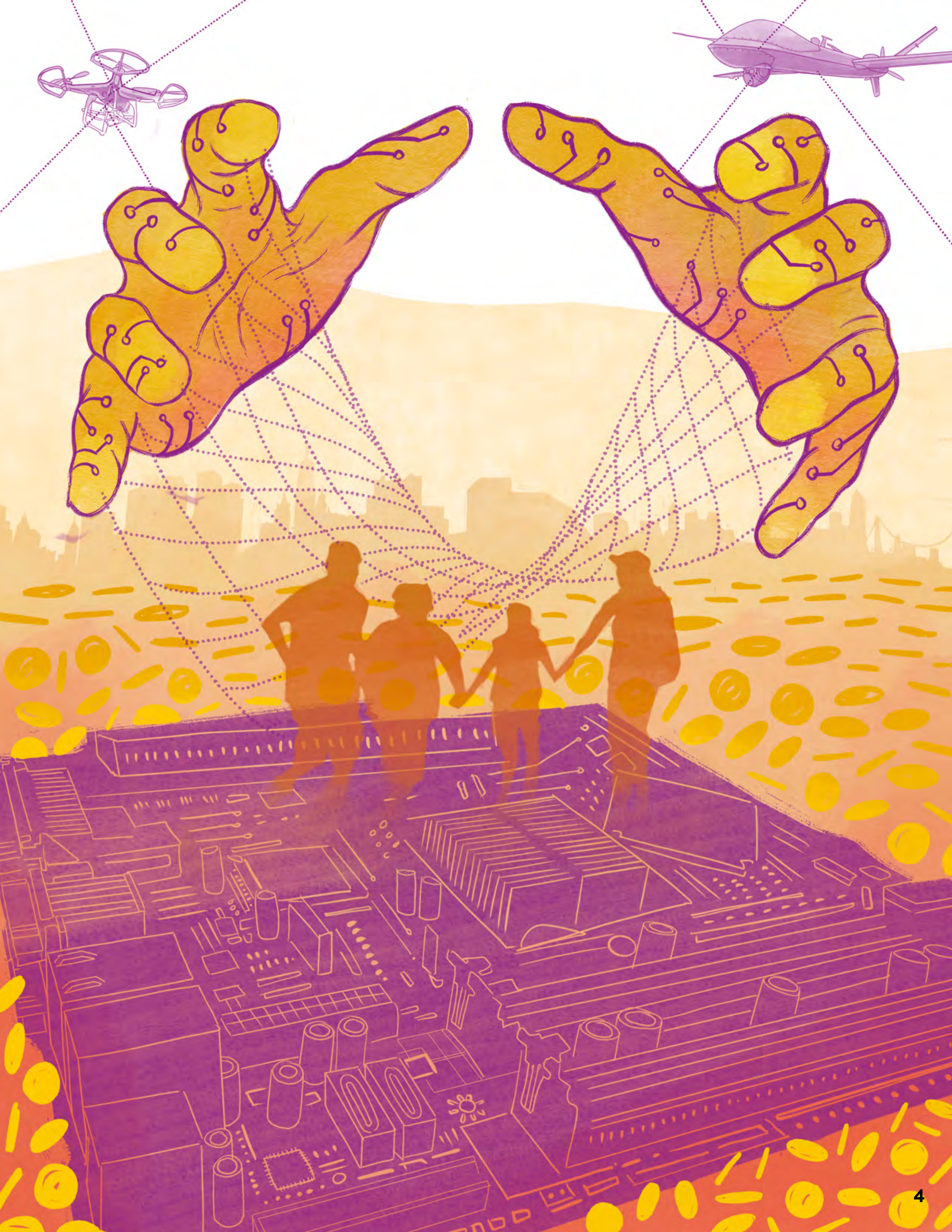
Rio Grande Valley No Border Wall Coalition is a multilingual and multi-generational collective of communities and partner organizations across the Rio Grande Valley who fight for a liberated region free of border walls and militarization.

Our organizations would like to thank the following organizations for their research and contributions to this report:

Empower, LLC conducts strategic corporate research in partnership with civil society organizations to advance human rights and corporate accountability, with a particular focus on technology, private capital, and grave crimes.

The Ida B. Wells JUST Data Lab undertakes research in partnership with community organizations to advance data justice — producing, using, and critiquing data to advance social justice. The Lab is based out of Princeton University and is run by founding director, Dr. Ruha Benjamin.

The Summer Immigration Institute of the Colorado College Department of Sociology, under the direction of Dr. Eric Popkin, trains students to conduct strategic research and engage directly in campaigns in support of community-led immigrant rights initiatives.



EXECUTIVE SUMMARY

A "digital border wall" has been steadily built along the U.S.-Mexico border for the last four presidential administrations, overseen by the Department of Homeland Security (DHS) and supported by Democrats and Republicans alike. The Biden administration plans to increase this digital border wall funding, marketing it as a "gentler" or "smarter" alternative to Trump's border wall. But these technologies are an extension of the Trump administration's border infrastructure buildup, not a break with it. Funding these border surveillance technologies will only continue the massive and unchecked expansion of government surveillance on immigrants and communities along the Southwest border and far into the interior.

Using government contracting data and interviews with migrants and border community residents, this report breaks down key pieces of the Southwest border's tech infrastructure into the following sections:

- **THE DIGITAL WALL:** border technology such as surveillance towers, drones, cameras, and automated license plate readers that compose the digital wall
- **BIOMETRICS**: biometric surveillance technology such as DNA, facial recognition, voice recognition, and iris scans used to surveil individuals
- **HACKING AND TRACKING:** phone and vehicle surveillance technologies

By exposing these technologies, this report aims to empower border activists, organizers, and residents to *challenge* the corporate tools used for border control and immigration enforcement by U.S. government agencies, and to more effectively advocate for a surveillance-free world.

What is the digital border wall? The digital border wall is made up of aerial drones, underground sensors, and surveillance towers amassed across hundreds of miles and capable of detecting humans, vehicles, and animals in all directions. It is the license plate scanners that catalogue every car in the border zone and the forensic kits that allow border patrol agents to retrieve personal data from these cars. It's the facial recognition, location tracking, and phone hacking tools available to a wide array of federal agencies operating in the borderlands. It is an attempt at total surveillance along the border and far into the interior, an effort by DHS to monitor and control everything that happens between the United States and Mexico under the justification of border enforcement.

Border surveillance is deadly. The hundreds of millions allocated by Congress only further migrant suffering and death. Border surveillance pushes migrants to take longer, more dangerous routes to avoid detection—leading to more deaths in the desert. Peer-reviewed research has shown that there is "significant correlation between the location of border surveillance technology, the routes taken by migrants, and the locations of recovered human remains in the southern Arizona desert."[1] U.S. Border Patrol reported finding the remains of more than 250 migrants who died along the U.S.-Mexico border in 2020 alone.[2] And, when people are detected by "smart" border technology and apprehended by U.S. Customs and Border Protection (CBP) or other law enforcement in U.S. territory, they are thrown into the same immigration enforcement dragnet that awaits all other undocumented immigrants—whether in private detention centers or shackled to electronic ankle monitors. The digital border is part of the same militarization logic, the same deportation logic, the same surveillance logic, and the same carceral logic that undergirds the entire immigration enforcement system. To call it a "smart" solution is to ignore the dirty cells that follow its use.

Border communities are the test subjects for surveillance everywhere. Border enforcement policies have long served as a testing ground for military-grade surveillance far into the interior. CBP expansively defines the border zone as any location that is 100 miles from a U.S. land or coastal border. Roughly two-thirds of the U.S. population lives within the 100-mile zone, including nine out of the 10 largest cities.[3] CBP drones have been deployed on Black Lives Matter protesters. in over a dozen cities nationwide.[4] The harms of border technology go far beyond the border and disproportionately impact Black, Indigenous, and communities of color.

The digital wall is a for-profit industry. Congress is giving billions of taxpayer dollars to military tech companies at the expense of migrants and border communities that have experienced deep historical disinvestment. The digital wall relies on cutting-edge, for-profit surveillance technologies developed by military contractors, Big Tech companies, and Silicon Valley start-ups. As border enforcement agencies become increasingly reliant on technology to monitor, detain, and deport immigrants, multi-million dollar contracts are being signed to develop tools for the region.

From 2017 to 2020, CBP alone received $743 million
from Congress for tech and surveillance.
In 2021, DHS received more than $780 million from Congress for the same.[5]

[1] Samuel Norton Chambers, et al. "Mortality, Surveillance and the Tertiary "Funnel Effect" on the U.S.-Mexico Border: A Geospatial Modeling of the Geography of Deterrence," *Journal of Borderland Studies*, Volume 36, 2021 (published online January 31, 2019)."

[2] Salvador Rivera, "Remains of More Than 250 Migrants Found Along Southern Border," Border Report, Jan. 11, 2021, https://www.borderreport.com/regions/texas/remains-of-more-than-250-migrants-found-along-southern-border-in-2020/.

[3] The Constitution in the 100-Mile Border Zone," ACLU, https://www.aclu.org/other/constitution-100-mile-border-zone.

[4] Zolan Kanno-Youngs, "U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance," *NY Times*, Jun. 19, 2020, https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html?smid=tw-share.

[5] Just Futures Law and Mijente, "Factsheet: The Dangers of A Tech Wall," https://justfutureslaw.org/wp-content/uploads/2021/04/Factsheet-on-Tech-Wall-and-CBP-Appropriations.pdf.

Invest in border communities, not the digital border wall. Communities along the U.S.-Mexico border have some of the highest poverty rates in the country due to systemic disinvestment.[6] Rather than pursue failed strategies, the Biden administration, and all administrations going forward, should instead invest in border communities and welcome immigrants. The question cannot continue to be: "How do we more efficiently deter migrants?" Investment will mean repairing areas of the border destroyed or harmed by the construction of the physical wall. It will mean ceasing, immediately, the deployment of physical systems like surveillance towers and drones that leave border communities and migrants surveilled and endangered. It will mean creating a humanitarian system for welcoming people seeking safety or a better life into the United States, a system that does not automatically impose surveillance and incarceration on those crossing a line in the sand.

We must oppose the digital border wall at all costs, just as we would oppose more deportations, more border patrol, or more detention centers. We must stand wholly against this steady embrace of technology by border enforcement, a naked attempt to amass millions in profits for military contractors while doing nothing to address migration for what it is: a natural, human response to violence, oppression, and poverty. We must expose, protest, and boycott the companies that profit from this border enforcement system, and we must demand that our lawmakers stop funding this inhumane response.

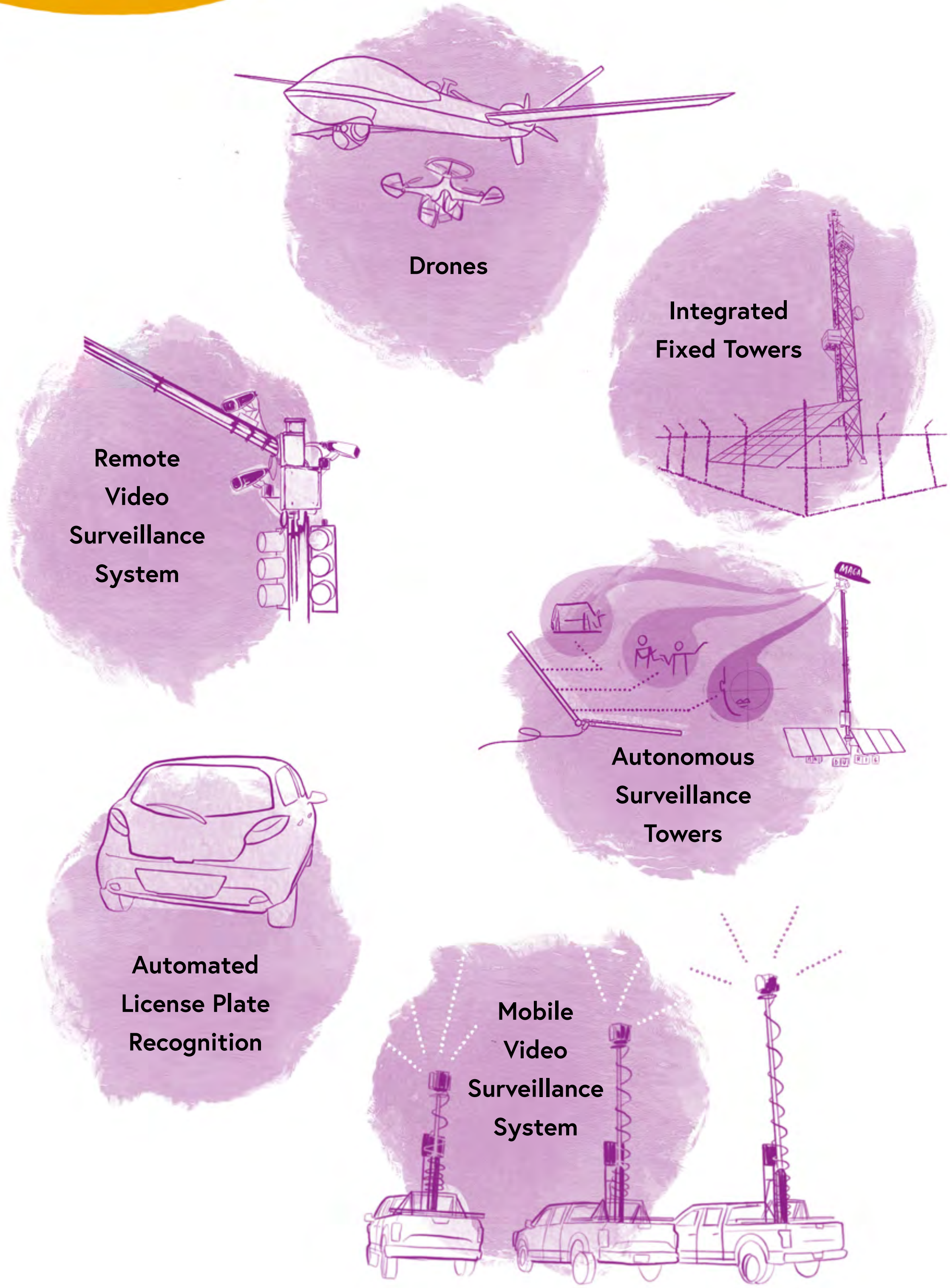
"As a lifelong resident of the Rio Grande Valley, I have witnessed how border militarization, including military tech, has overwhelmed our communities. Million-dollar surveillance towers are getting built in border communities like the Colonias where the government has neglected basic infrastructure like electricity, water, and sewage systems. Our government's gross priorities are that of militarization and profit, not people and community. We must demand public officials to treat us with dignity and to invest in us, to create community opportunities not centered on brutality or self-destruction."

- Roberto Lopez, No Border Wall Coalition & Texas Civil Rights Project

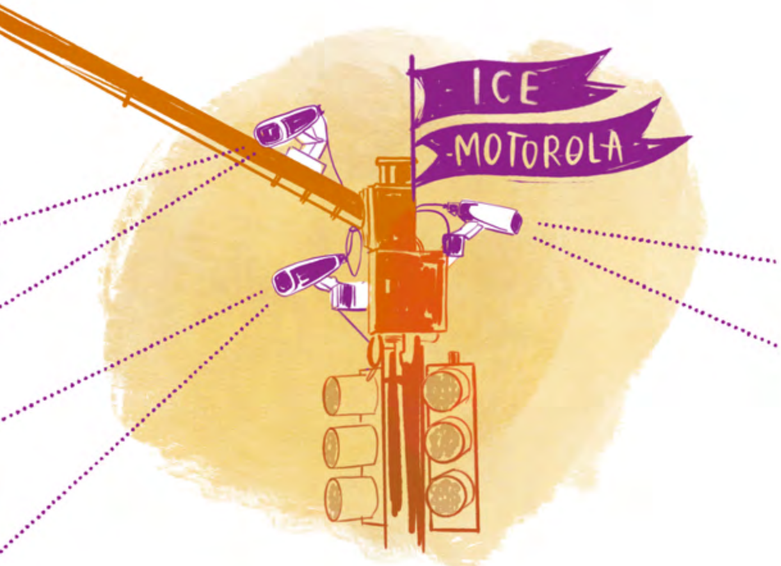
[6] "Latest Census Data Shows Poverty Rate Highest at Border, Lowest in Suburbs," *Texas Tribune*, Jan. 19, 2016, https://www.texastribune.org/2016/01/19/poverty-prevalent-on-texas-border-low-in-suburbs/; "Inside Texas' Border Communities: What are Colonias?," MHP Salud, https://mhpsalud.org/inside-texas-border-communities-colonias/

DIGITAL WALL

This section details key hardware used in Southwest border surveillance. These technologies are actively deployed at the border and oftentimes the most visible to the naked eye.


Drones
Integrated Fixed Towers
Remote Video Surveillance System
MAGA
Autonomous Surveillance Towers
Automated License Plate Recognition
Mobile Video Surveillance System

AUTOMATED LICENSE PLATE RECOGNITION



Automated License Plate Recognition (ALPR) is a surveillance technology consisting of cameras that capture data about vehicles and their passengers, including the date, time, and location of the picture taken. Fixed atop streetlights, telephone poles, overpasses, and police cars, these cameras are capable of logging data on passing and parked vehicles. This data can be used to determine the travel patterns of individual drivers. Most importantly, the plate data can be matched with a car's owner to track their movement, and stored and shared among different law enforcement agencies.

CBP uses ALPR at border crossing lanes and Border Patrol checkpoints further inland. The technology allows agents to check information on vehicle owners in real-time.[7] The agency has a contract worth $54.6 million for ALPR equipment, provided by Chicago-based company Motorola Solutions.[8]

Meanwhile, U.S. Immigration and Customs Enforcement (ICE) subscribes to a private license database and information-sharing system run by Vigilant Solutions, a subsidiary of the same company. This database is a notorious platform for backdoor sharing of personal and location information on individuals between local police and ICE, both intentionally and unintentionally, sometimes in violation of state law.[9] ICE uses this for-profit platform through an agreement with data broker Thomson Reuters worth $22.8 million through 2026.[10] Through this platform, ICE had access, as of 2019, to over 5 billion license plate records from private businesses, as well as 1.5 billion data points from over 80 law enforcement agencies across the country.[11]

[7] DHS Privacy Impact Assessment, CBP License Plate Reader Technology, July 6, 2020.

[8] CBP contracting data, Delivery Order HSBP1017J00223.

[9] Yesenia Amaro, "Tulare Police Department says it didn't know it was sharing data with ICE, apologizes," *Fresno Bee*, March 18, 2019, www.fresnobee.com/news/local/article228102949.html#storylink=cpy.

[10] ICE contracting data, Definitive Contract 70CMSD21C00000002.

[11] "Internal Docs Show How ICE Gets Surveillance Help From Local Cops," *Wired*, March 13, 2019, www.wired.com/story/ice-license-plate-surveillance-vigilant-solutions.

> *"Now, they have those sensors everywhere. They have helicopters throughout the night. At the river they have drones, they have infrared rays, they have a lot of surveillance. It's really spectacular the type of surveillance they have. There are all these sensors and you don't know where they are. If you stop somewhere and there's a sensor, it shoots the signal to the office and it alerts them. They have a very robust surveillance technology at the border."*
>
> *- Anonymous*

INTEGRATED FIXED TOWERS

There are several surveillance tower systems along the Southwest border, including the Integrated Fixed Towers (IFTs) developed by Israeli military contractor Elbit Systems. These structures are 80 to 140 feet tall and are equipped with day and night cameras and a radar that can identify people six miles away. The towers send this data to a remote command and control center system called TORCH, which Elbit first developed for Israel's separation wall in the West Bank.[12] On the U.S.-Mexico border, immigration agents use the information to track and apprehend people. In 2014, the company signed a contract worth up to $239 million for the development of this tower system.[13] As of 2019, there were 55 of these towers deployed in Arizona.[14]

Institutions including Norway's national pension fund system have divested from Elbit Systems due to "serious violations of fundamental ethical norms as a result of the company's integral involvement in Israel's construction of a separation barrier on occupied territory" in the West Bank.[15]

[12] Will Parrish, "The U.S. Border Patrol And An Israeli Military Contractor Are Putting A Native American Reservation Under 'Persistent Surveillance,'" *The Intercept*, August 25, 2019, https://theintercept.com/2019/08/25/border-patrol-israel-elbit-surveillance.

[13] CBP contracting data, Definitive Contract HSBP1014C00004.

[14] Will Parrish, "The U.S. Border Patrol And An Israeli Military Contractor Are Putting A Native American Reservation Under 'Persistent Surveillance,'" *The Intercept*, August 25, 2019, https://theintercept.com/2019/08/25/border-patrol-israel-elbit-surveillance.

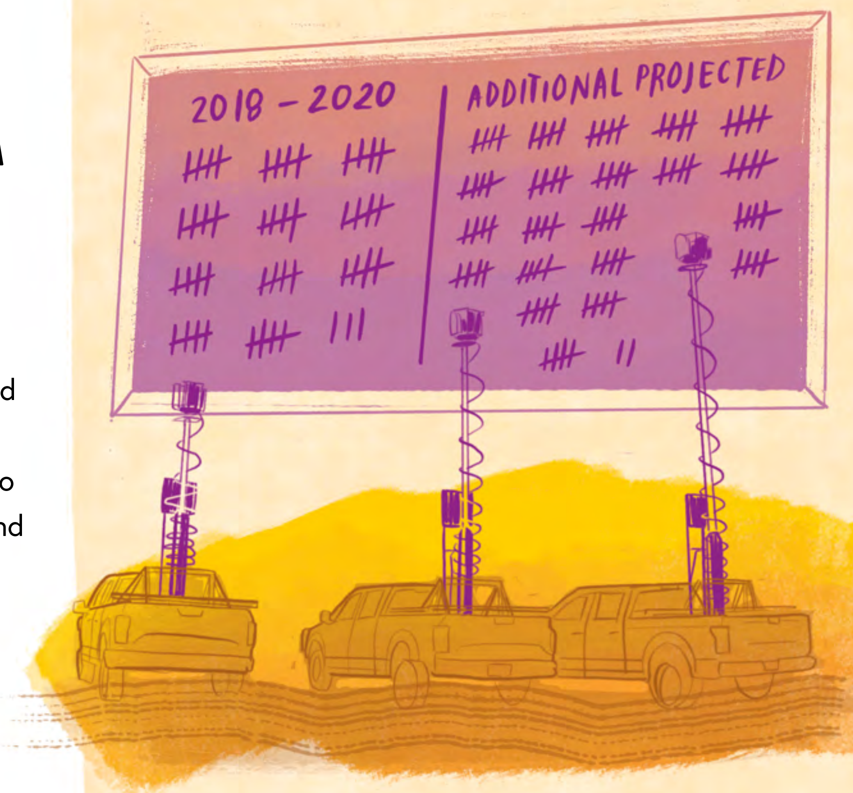
[15] Elizabeth Adams, "Norway's Pension Fund Drops Israel's Elbit," *Wall Street Journal*, September 3, 2009, www.wsj.com/articles/SB125197496278482849.

REMOTE VIDEO SURVEILLANCE SYSTEM

The Remote Video Surveillance System (RVSS) encompasses a series of smaller, relocatable surveillance towers along the Southwest and Northern borders. Some cameras are also mounted on tall buildings or other structures. The RVSS system uses color and infrared cameras with video analytics that allow CBP to monitor both urban and rural areas along the border.

This system has also been used for purposes of domestic political surveillance. In 2017, CBP stationed one of its RVSS towers in San Diego to monitor political opposition to the building of prototypes for the physical border wall, citing the "emerging threat of demonstrations."[16]

As of 2021, CBP had built 368 RVSS towers in locations ranging from San Diego to the Rio Grande Valley to the Northern U.S. border.[17] Military contractor General Dynamics has a contract worth $153 million through 2023 to expand the system.[18]



MOBILE VIDEO SURVEILLANCE SYSTEM

Another kind of tower used for purposes of border surveillance is the Mobile Video Surveillance System (MVSS). Each MVSS unit consists of a 4x4 truck with telescoping poles in the bed that extend up to 35 feet in the air, outfitted with thermal and video cameras and a laser illuminator. They can record video up to six miles away. The drivers of these vehicles are often military personnel, in addition to CBP agents.[19]

Between 2018 and February 2020, CBP deployed 58 MVSS units along the Texas border,[20] with plans to implement 165.[21] The company building them under an $80 million contracting vehicle[22] is Tactical Micro, a subsidiary of the Tempe, Arizona-based Benchmark Electronics.

The MVSS platform also uses geospatial analytics software from PureTech Systems of Phoenix as its central command and control system within the vehicle.[23]

[16] Will Parrish, "The U.S. Border Patrol And An Israeli Military Contractor Are Putting A Native American Reservation Under 'Persistent Surveillance,'" *The Intercept,* August 25, 2019, https://theintercept.com/2019/08/25/border-patrol-israel-elbit-surveillance.

[17] Ibid.

[18] CBP contracting documents, Definitive Contract HSBP1013C00042.

[19] DHS Office of Inspector General, "CBP Has Improved Southwest Border Technology, but Significant Challenges Remain," February 23, 2021, www.oig.dhs.gov/sites/default/files/assets/2021-02/OIG-21-21-Feb21.pdf.

[20] Ibid.

[21] Government Accountability Office, "Southwest Border Security: Border Patrol Is Deploying Surveillance Technologies but Needs to Improve Data Quality and Assess Effectiveness," November 2017.

[22] CBP contracting data, IDIQ HSBP1016D00002.

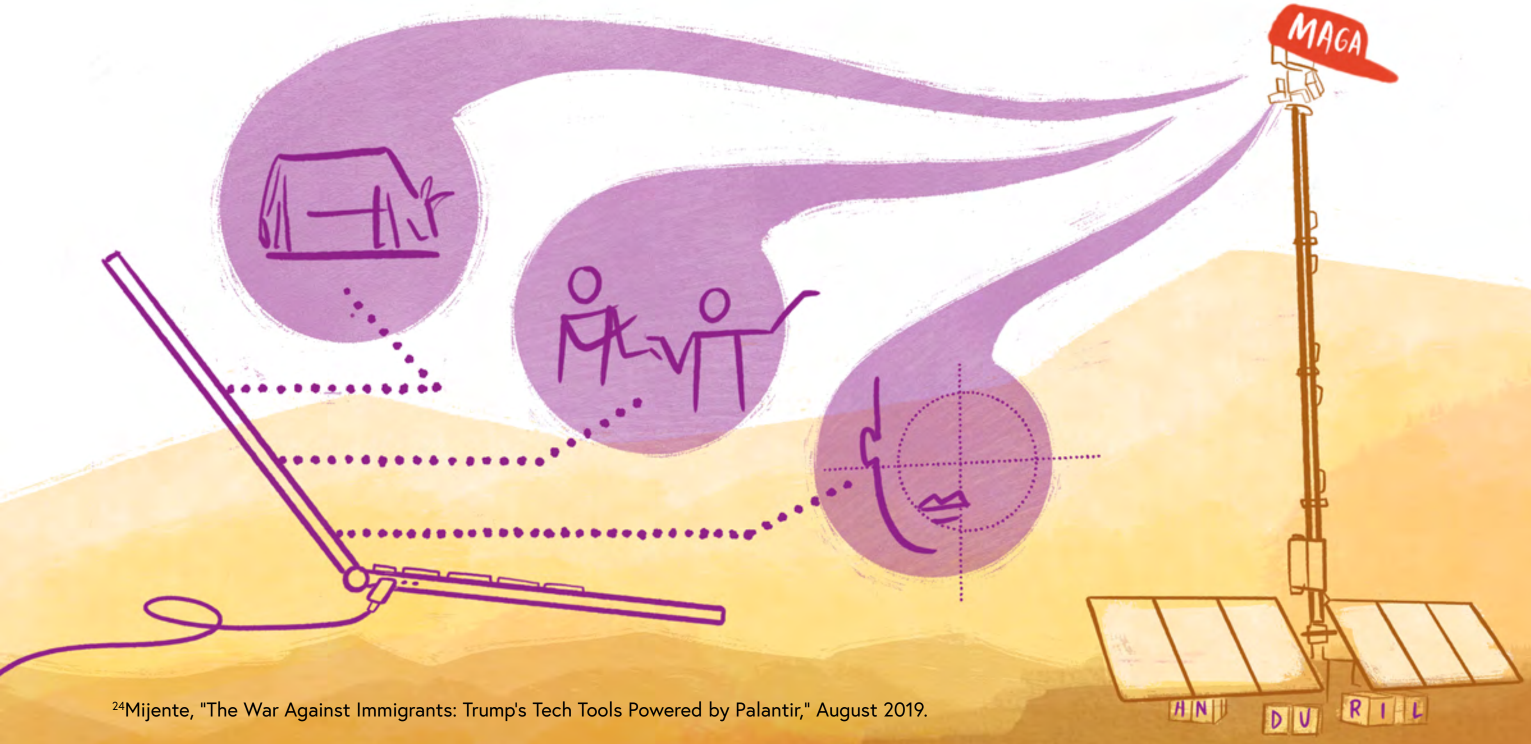
[23] PureTech Systems, "PureTech Systems' Delivering on Orders of its PureActiv Software providing Rapidly Deployable Advanced Surveillance Technology to U.S. Border Patrol," press release, July 29, 2020, www.puretechsystems.com/pureactiv-to-border-patrol-release.

AUTONOMOUS SURVEILLANCE TOWERS

The newest border surveillance towers are also the most high-tech. The Autonomous Surveillance Towers developed by Anduril Industries use Artificial Intelligence to identify and classify items of interest, distinguishing between people and livestock, without the direct control of a human operator. They are also capable of identifying and capturing human faces, though contracting documents specify that this function is only to be used for vendor training purposes. The relocatable towers are 33 feet tall and suited to work in remote environments with little maintenance, since they operate off the grid and around the clock, using solar panels for energy.

Anduril was founded in 2017 by Trump donor Palmer Luckey, with funding from Trump donor Peter Thiel, and staffed by executives from Thiel's Palantir Technologies.[24] Palantir provides key technologies used by ICE in workplace raids, and to target individuals for deportation.[25]

Four Anduril towers were originally piloted in San Diego in 2018. Since then, 56 more towers have been added, and CBP plans to install 200 towers by fiscal year 2022.[26] In July 2020, Anduril was awarded a contract worth $250 million through 2025 for this project.[27]

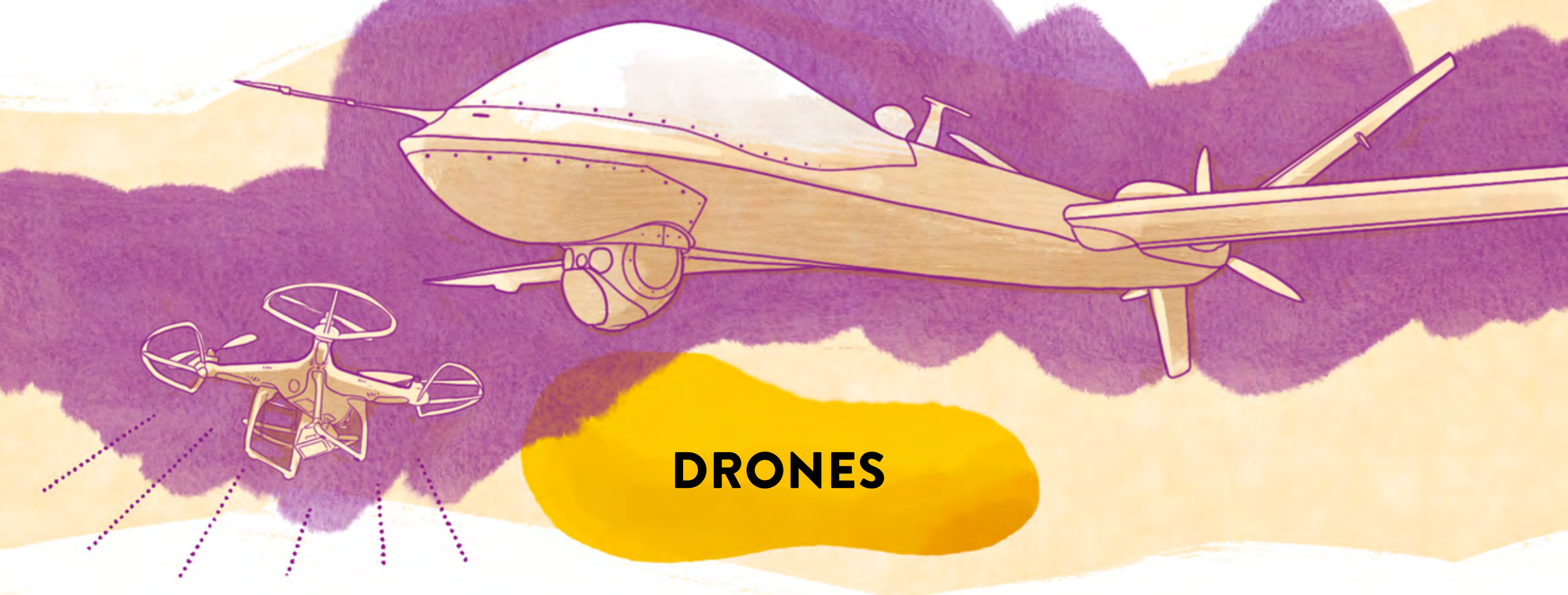


[24] Mijente, "The War Against Immigrants: Trump's Tech Tools Powered by Palantir," August 2019.

[25] Ibid.

[26] CBP, "CBP'S Autonomous Surveillance Towers Declared A Program Of Record Along The Southwest Border," last modified February 3, 2021, www.cbp.gov/newsroom/national-media-release/cbp-s-autonomous-surveillance-towers-declared-program-record-along.

[27] CBP contracting documents, IDIQ 70B02C20D00000019.



DRONES

CBP has used drones to surveil the Southwest border for years, upgrading and expanding drone fleets as new technology and more funding becomes available. In 2006, the agency began using Predator B drones, which weigh 5,000 pounds and measure nearly 36 feet.[28] These are a version of the U.S. military's reaper drone, each costing $17 million to purchase and $12,255 per flight hour to operate.[29] Each time one of these drones is used to apprehend individuals at the border, it costs an estimated $32,000.[30] Private company General Atomics, of San Diego, currently has a contract worth $250 million through 2023 for their operation and maintenance.[31]

More recently, CBP has begun contracting smaller drones known as small unmanned aerial systems (sUAS), weighing less than 55 pounds. These drones are able to collect images and video, and some can also sense human movement. Agents use them, in particular, to track people in mountainous and hard-to-access terrain.

By 2020, CBP was already using more than 135 drones, with plans to procure 460. Nearly 600 operators were trained to fly them, and the agency aimed to double that number in 2021 with a training program in West Virginia.[32] These machines can fly autonomously and have the ability to surreptitiously monitor what's happening on the ground. They are controlled through handheld devices. Since 2016, CBP has expressed interest in developing drones with facial recognition capabilities.[33]

Manufacturers of small border drones include AeroVironment, FLIR Systems, and Lockheed Martin, all with multi-million dollar contracts.

[28] David Bier, "Drones on the Border: Efficacy and Privacy Implications," Cato Institute, 2021, www.cato.org/immigration-research-policy-brief/drones-border-efficacy-privacy-implications.

[29] Ibid.

[30] Shirin Ghaffary, "The "smarter" wall: How drones, sensors, and AI are patrolling the border," Recode, February 7, 2020, www.vox.com/recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai.

[31] CBP contracting data, Definitive Contract 70B02C18C00000040.

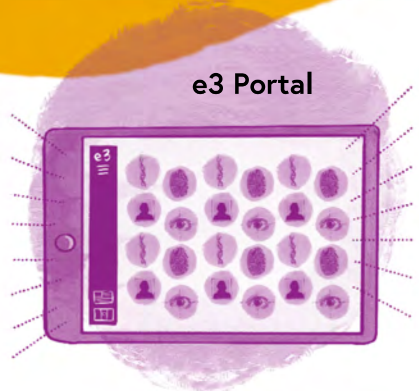
[32] John Davis, "Small but Mighty," CBP, www.cbp.gov/frontline/cbp-small-drones-program.

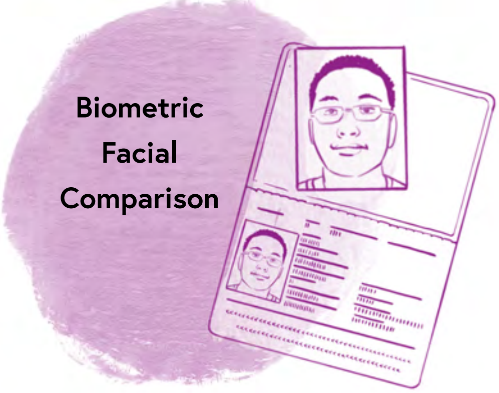
[33] Russell Brandom, "The US Border Patrol is trying to build face-reading drones," *The Verge*, April 6, 2017, www.theverge.com/2017/4/6/15208820/customs-border-patrol-drone-facial-recognition-silicon-valley-dhs.

BIOMETRICS

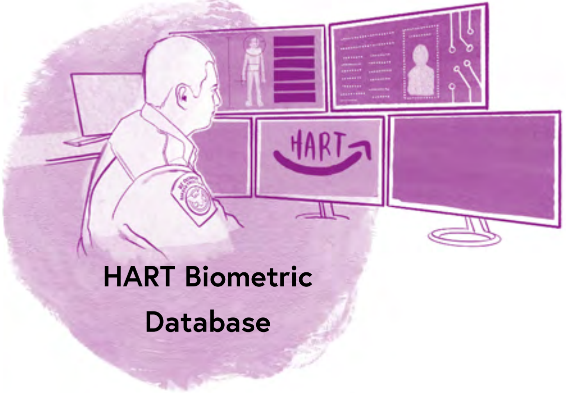
Biometrics are physical characteristics used to identify people, such as fingerprints, DNA, facial recognition, voice recognition, and iris scans. DHS is rapidly expanding the types of biometrics it collects and the places it collects them, often without permission. CBP has run pilot programs of iris scans at pedestrian border crossings and facial recognition of car passengers. Facial recognition is now a widespread practice at airports. Since 2020, ICE and CBP have begun collecting DNA samples, with no consent required, from all non-U.S. citizens apprehended by the two agencies, and storing their DNA profiles in the FBI's Combined DNA Index System (CODIS).[34]

This is profoundly concerning, due both to privacy concerns and to the demonstrated technical shortcomings of biometric technology. Facial recognition use by police has already resulted in false positives and wrongful arrests, particularly of black men.[35] DHS bluntly acknowledges that there is a risk its "facial image matching results may be inaccurate or result in a disproportionate impact to certain populations," due to inherent biases based on factors including race, sex, and age.[36]


e3 Portal


Biometric Facial Comparison

CBP One Application



HART Biometric Database

[34] Applicable to persons between 14 and 79 years of age. See: CBP, "CBP to Meet Legal Requirement to Collect DNA Samples from Certain Populations of Individuals in Custody," press release, December 3, 2020, www.cbp.gov/newsroom/national-media-release/cbp-meet-legal-requirement-collect-dna-samples-certain-populations

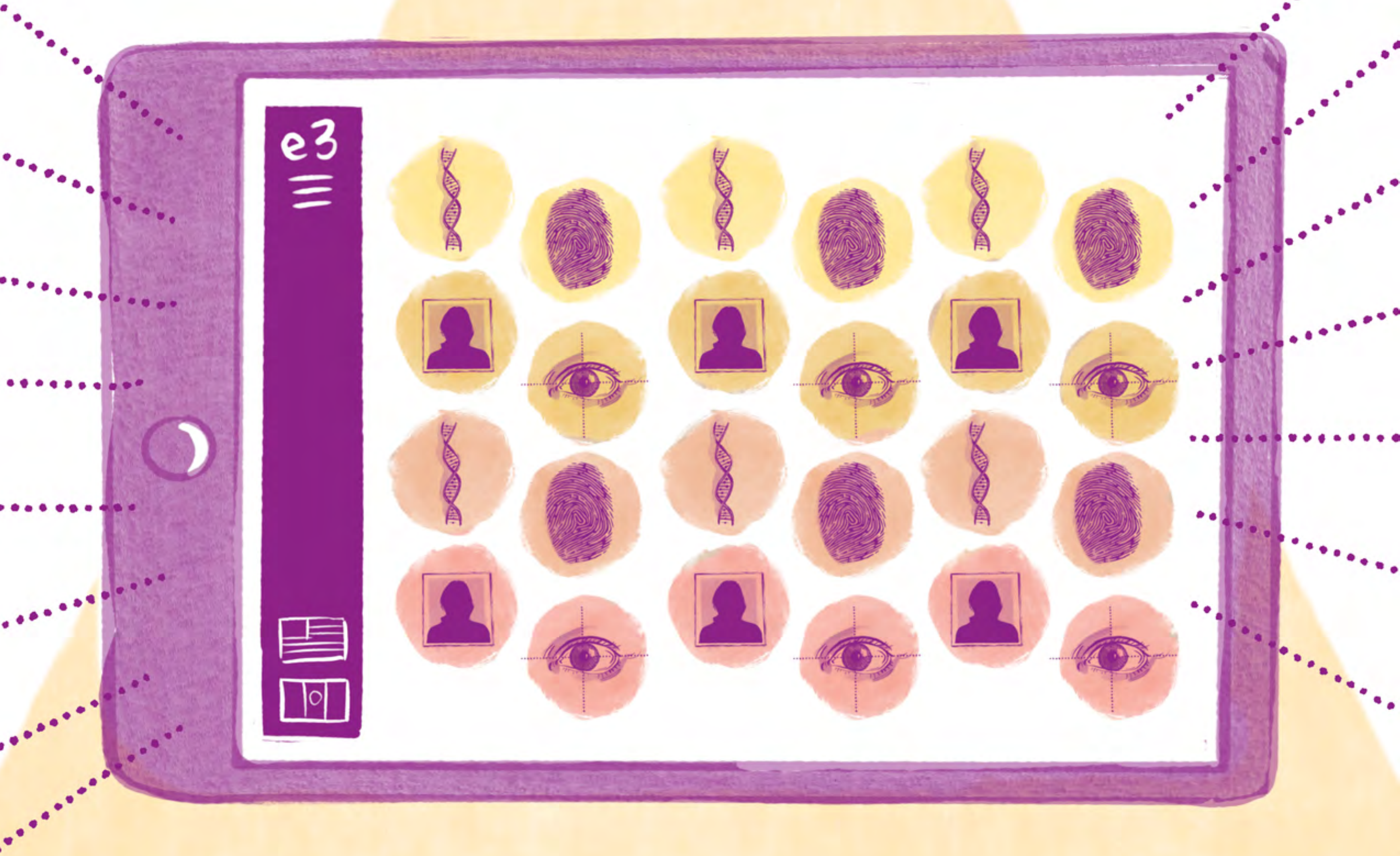
[35] See, for example: Adi Robertson, "Detroit man sues police for wrongfully arresting him based on facial recognition," *The Verge*, April 13, 2021, www.theverge.com/2021/4/13/22382398/robert-williams-detroit-police-department-aclu-lawsuit-facial-recognition-wrongful-arrest.

[36] DHS, DHS/OBIM/PIA-004, "Homeland Advanced Recognition Technology System (HART) Increment 1 PIA," February 24, 2020.

E3 PORTAL

When CBP agents apprehend someone in the border region, in addition to collecting DNA samples for storage by the FBI, they also take fingerprints, a facial photograph, and an iris image, all to be transmitted in real time to the DHS biometric database. Agents use a suite of applications known as the e3 portal to collect these biometrics.[37]

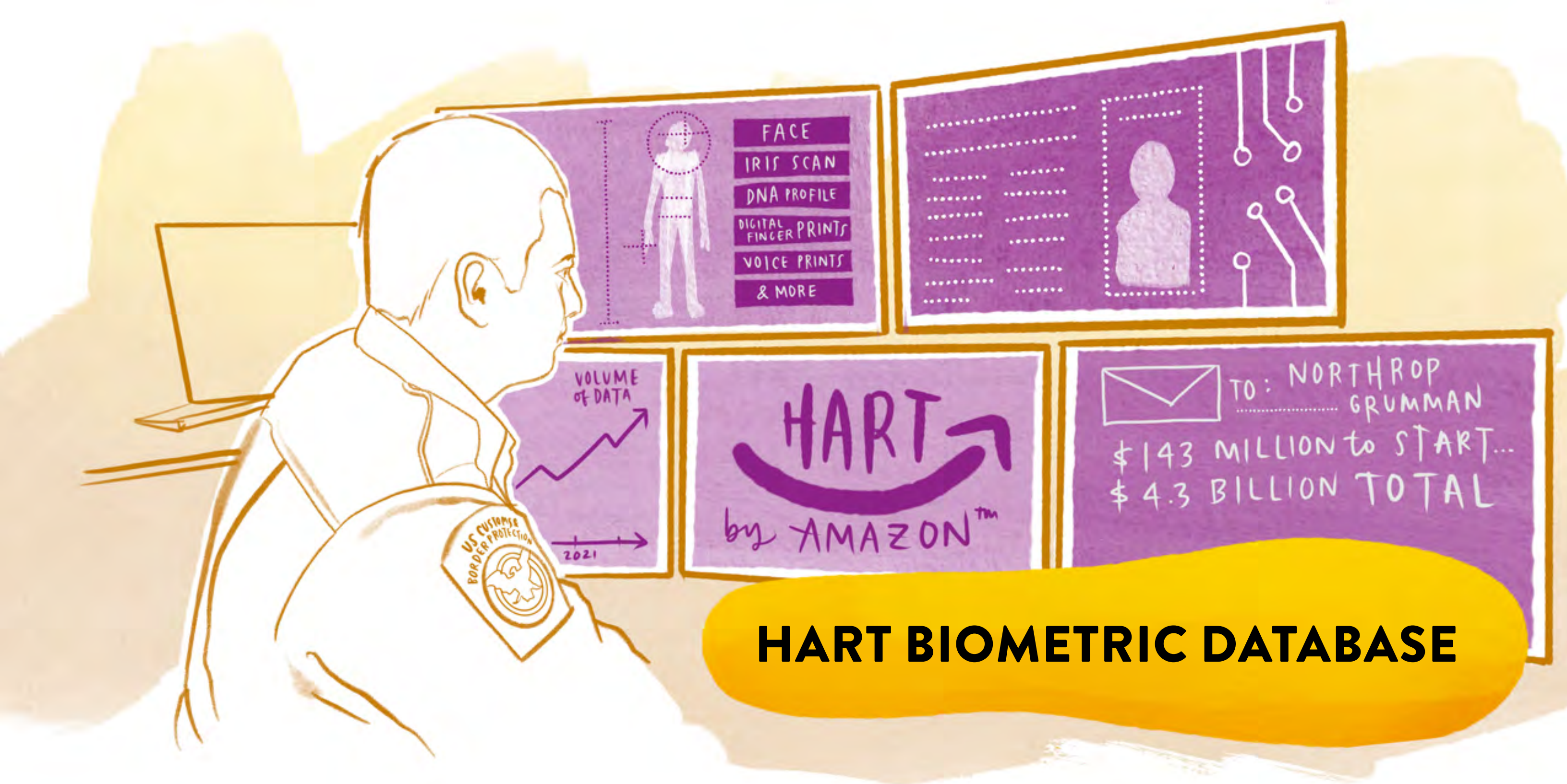
The e3 portal sends fingerprints and facial and iris images directly to ICE's case management system for Enforcement and Removal Operations (ERO) and to the DHS-wide IDENT database, which is the agency's current biometric storage system. This repository holds information about more than 260 million people and can process more than 350,000 biometric transactions per day.[38] Through binational information sharing agreements with Mexico, this database also contains bulk biometric information on people apprehended by Mexican immigration authorities anywhere in that country.[39]



[37] See relevant Privacy Impact Assessments at www.dhs.gov/publication/cbp-portal-e3-enforceident.

[38] DHS, Biometrics, www.dhs.gov/biometrics.

[39] Mijente, Immigrant Defense Project, and Just Futures Law, "Who's Behind ICE?: The Tech and Data Companies Fueling Deportations," September 2018.



HART BIOMETRIC DATABASE

The Homeland Advanced Recognition Technology System (HART) is a centralized database of biometric data that will replace the automated biometric identification system (IDENT) currently used by DHS. Hosted by Amazon Web Services, the new system will aggregate, link, and compare facial recognition images, DNA profiles, iris scans, digital fingerprints, and voice prints on unique profiles of hundreds of millions of people.[40]
The planned database will collect this invasive personal data from diverse federal agencies like ICE, CBP, Federal Bureau of Investigation (FBI), and the Department of Defense, as well as from local and state law enforcement, and from foreign governments including Mexico, the Northern Triangle countries of Central America, and the Five Eyes alliance.[41]

HART is a dramatic expansion of the biometric architecture underlying the Secure Communities program, which relied on automated fingerprint sharing between local law enforcement and ICE. Secure Communities was launched in March 2008 and triggered a sharp increase in deportations during the early years of the Obama administration. By the time of the program's first suspension in November 2014, it was already responsible for an estimated 450,000 deportations.[42] If the new HART database is implemented, ICE's capacity to exploit biometric matching will create the conditions for an unprecedented polimigra dragnet.

Military contractor Northrop Grumman has been awarded a $143 million contract to develop the first increment of this system, estimated to cost a total of $4.3 billion.[43]

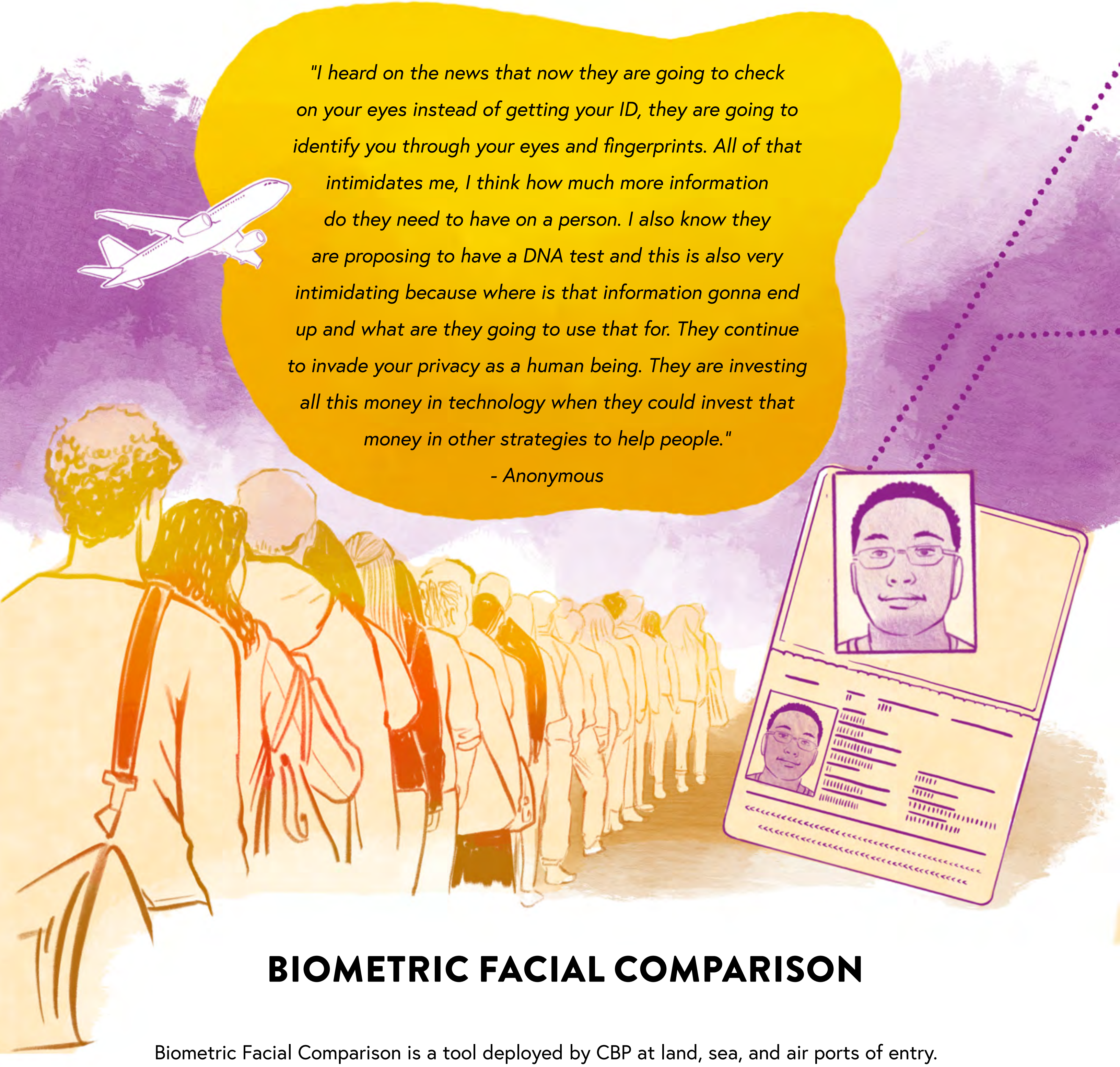
[40] U.S. Department of Homeland Security, DHS/OBIM/PIA-004, "Homeland Advanced Recognition Technology System (HART) Increment 1 PIA," February 24, 2020.

[41] Guatemala, Honduras, El Salvador, the United Kingdom, Canada, Australia, and New Zealand.

[42] Chloe East, "Secure Communities: Broad Impacts of Increased Immigration Enforcement," EconoFact, January 13, 2020, https://econofact.org/secure-communities-broad-impacts-of-increased-immigration-enforcement.

[43] "DHS Annual Assessment: Most Acquisition Programs are Meeting Goals but Data Provided to Congress Lacks Context for Effective Oversight," GAO, January 2021, p. 38; https://www.gao.gov/assets/gao-21-175.pdf.

> *"I heard on the news that now they are going to check on your eyes instead of getting your ID, they are going to identify you through your eyes and fingerprints. All of that intimidates me, I think how much more information do they need to have on a person. I also know they are proposing to have a DNA test and this is also very intimidating because where is that information gonna end up and what are they going to use that for. They continue to invade your privacy as a human being. They are investing all this money in technology when they could invest that money in other strategies to help people."*
>
> *- Anonymous*



BIOMETRIC FACIAL COMPARISON

Biometric Facial Comparison is a tool deployed by CBP at land, sea, and air ports of entry. The facial comparison system compares an existing passport or visa photo to a traveler's photo, taken on the spot.[44] CBP has expanded the system to include biometric collection upon both entry and exit of travelers. Information collected via biometric facial comparison is stored in the IDENT biometric database and retained for 15 years for U.S. citizens and lawful permanent residents, and 75 years for all others.[45]

[44] CBP, Biometrics, **https://biometrics.cbp.gov**.

[45] DHS, "Privacy Impact Assessment for the Traveler Verification Service," November 14, 2018.

CBP ONE APPLICATION

The CBP One mobile application was launched in October 2020 by CBP. Though it has various functions, one key purpose is processing asylum seekers before they arrive at land ports of entry on the Southwest border. The app utilizes facial recognition and geolocation, and collects extensive personal information on asylum seekers.

CBP has recruited NGOs including the International Rescue Committee and the United Nations Refugee Agency, or UNHCR, to use the app for asylum seekers.

The Trump administration's Migrant Protection Protocols, also known as the "Remain in Mexico" policy, forced some 70,000 people to wait in Mexico for immigration hearings. On top of this, the Trump administration used a public health law known as Title 42 to close the border to nonessential travel during the coronavirus pandemic, worsening the situation for asylum seekers. The CBP One app is meant to address this crisis, but creates new privacy concerns, as it extends the collection of biometric and personal data beyond the physical borders of the United States.[46]

Information that can be logged into the app includes phone number, employment and family information, marital status, individuals traveling together, permanent address abroad, and destination in the United States, as well as a photograph to be run through CBP biometric records. CBP does not store the photograph, but it does store all case and biographic information on the Amazon cloud for 365 days.

The further technologizing of the asylum seeking process allows for more tracking of individuals and more invasive information sharing. Furthermore, facial recognition alone, shown to be an imperfect technology, is a determinant in whether asylum seekers are allowed to enter the U.S.

[46] Molly O'Toole, "Exclusive: Biden has quietly deployed an app for asylum seekers. Privacy experts are worried," *Los Angeles Times,* June 4, 2021, www.latimes.com/politics/story/2021-06-04/asylum-bidens-got-an-app-for-that-with-privacy-risks-and-surveillance-beyond-border

HACKING AND TRACKING

Hacking technologies are used by CBP to obtain personal information for investigation or immigration policing purposes, often sharing it with other government entities including state, local and foreign agencies. Earlier this year, a federal appeals court ruled that CBP does not need a warrant to search people's mobile devices who are entering the country, whether or not they are U.S. citizens.[47] Agents have the legal authority to go through any device within 100 miles of the border and to take devices away from travelers for up to five days without providing justification.[48]

CBP also has the ability to physically track people in the border region, using both visible technology, such as drones, and invisible methods such as location tracking.

Venntel Location Tracking

Mobile Phone Hacking

Vehicle Forensic Kits

Intelligent Computer Assisted Detection

[47] Nate Raymond, "U.S. border agents do not need warrants to search digital devices, court rules," *Reuters*, February 20, 2021, www.reuters.com/article/us-usa-immigration-privacy/u-s-border-agents-do-not-need-warrants-to-search-digital-devices-court-rules-idUSKBN2AA2AL

[48] Cynthia McFadden et al. "American Citizens: U.S. Border Agents Can Search Your Cellphone," NBC News, March 13, 2017, www.nbcnews.com/news/us-news/traveling-while-brown-u-s-border-agents-can-search-your-n732746.

MOBILE PHONE HACKING

Border agents
have multiple proprietary technologies at their disposal to hack into people's mobile phones. These include the Israeli company Cellebrite, the Atlanta-based Grayshift, and Magnet Forensics of Canada. Each of these companies has various contracts with CBP and ICE for hacking software that serves different purposes. For example, Grayshift's Graykey software tool can hack into locked iPhones. Cellebrite also has the power to break through some lockscreens.[49]

CBP searched 40,913 electronic devices at the border in 2019 alone.[50] Many such warrantless searches have targeted journalists, lawyers, and activists during secondary inspection at ports of entry, whose phones are hacked as they are submitted to interrogation and sometimes held in detention cells for hours.[51]

[49] Thomas Brewster, "US Immigration Splurged $2.2 Million On Phone Hacking Tech Just After Trump's Travel Ban," *Forbes*, April 13, 2017, www.forbes.com/sites/thomasbrewster/2017/04/13/post-trump-order-us-immigration-goes-on-mobile-hacking-spending-spree/?sh=5ad0665fa1fc.

[50] Nate Raymond, "U.S. Border Agents Do Not Need Warrants to Search Digital Devices, Court Rules," *Reuters*, Thomson Reuters, February 10, 2021, www.reuters.com/article/us-usa-immigration-privacy/u-s-border-agents-do-not-need-warrants-to-search-digital-devices-court-rules-idUSKBN2AA2AL

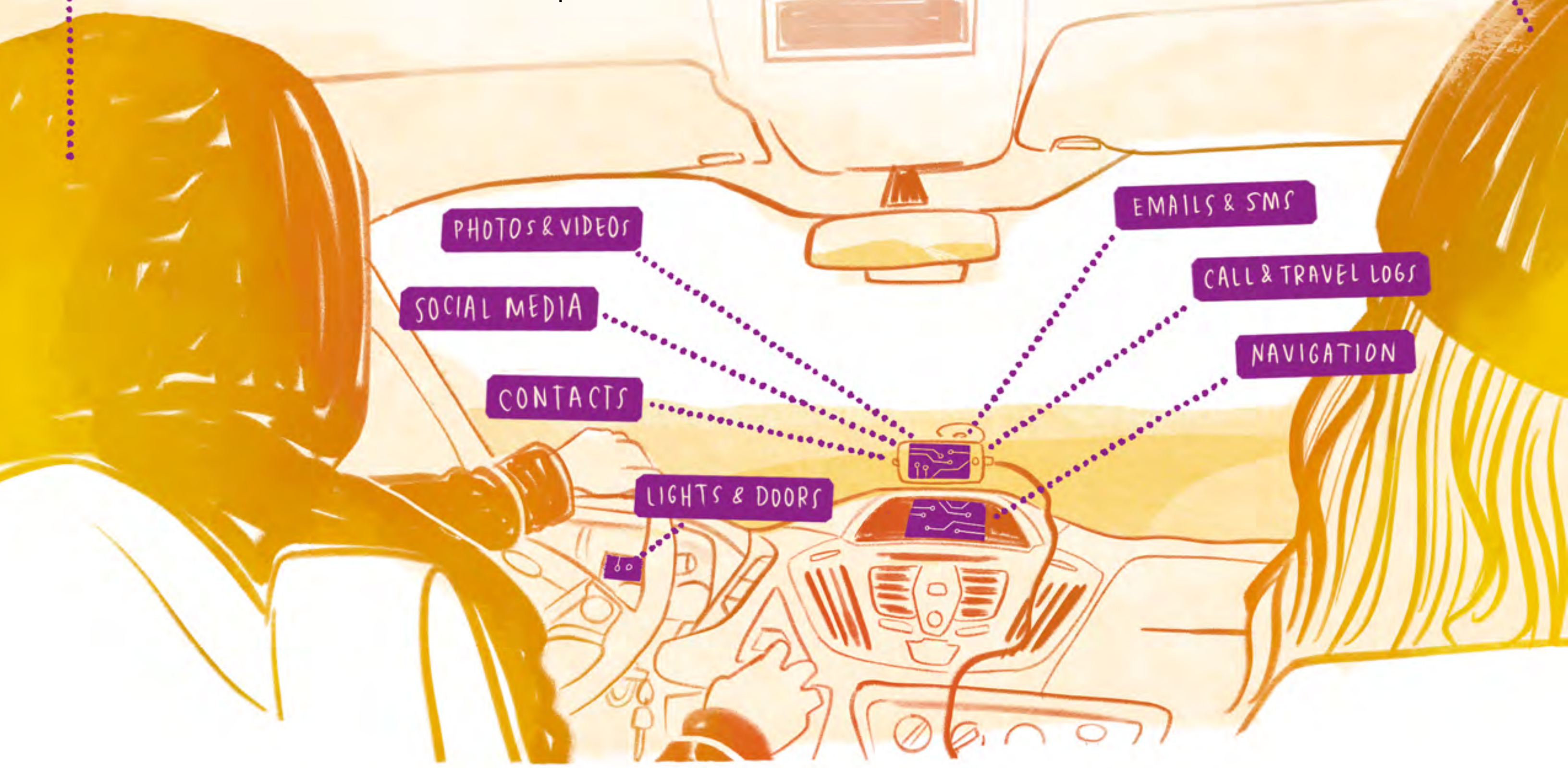
[51] Ryan Devereaux, "Journalists, Lawyers, and Activists Working on the Border Face Coordinated Harassment From U.S. and Mexican Authorities," *The Intercept*, February 8, 2019, https://theintercept.com/2019/02/08/us-mexico-border-journalists-harassment.

VEHICLE FORENSICS KITS

Vehicle forensics kits are a new hacking technology that can hack personal information directly from vehicles' infotainment and navigation systems, even accessing contact lists and call logs from any synchronized mobile devices. These kits are manufactured by Berla Corporation, a Maryland company that has partnered with Swedish mobile forensics company MSAB to provide the service to CBP.[52]

The type of information that can be obtained from vehicles is vast and invasive. Data that can be extracted with Berla technology includes recent destinations, favorite locations, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and navigation history. Some vehicles even record when and where their lights are turned on and which doors are opened and closed at a specific location.[53]

While vehicle forensics kits can be used without a warrant, federal immigration authorities also use warrants to obtain location data of specific vehicles directly from GM, as well as data brokers Geotab and Spireon.[54]



[52] Thomas Brewster, "US Immigration Splurged $2.2 Million On Phone Hacking Tech Just After Trump's Travel Ban," *Forbes*, April 13, 2017, www.forbes.com/sites/thomasbrewster/2017/04/13/post-trump-order-us-immigration-goes-on-mobile-hacking-spending-spree/?sh=5ad0665fa1fc

[53] Nate Raymond, "U.S. Border Agents Do Not Need Warrants to Search Digital Devices, Court Rules," *Reuters*, Thomson Reuters, February 10, 2021, www.reuters.com/article/us-usa-immigration-privacy/u-s-border-agents-do-not-need-warrants-to-search-digital-devices-court-rules-idUSKBN2AA2AL

[54] Ryan Devereaux, "Journalists, Lawyers, and Activists Working on the Border Face Coordinated Harassment From U.S. and Mexican Authorities," *The Intercept*, February 8, 2019, https://theintercept.com/2019/02/08/us-mexico-border-journalists-harassment.

VENNTEL LOCATION TRACKING

Venntel is a private company that aggregates location data from smartphone apps and sells it to federal government agencies including ICE and CBP. These agencies have not been transparent about their use of the data, but people familiar with their practices have explained that ICE uses the location data to help identify immigrants for arrest, and that CBP uses the data to track cell phone activity in remote stretches of the Southwest border region.[55]

A 2018 Privacy Impact Assessment indicates that "CBP may use commercially available location data acquired from a data provider in order to detect the presence of individuals in areas between Ports of Entry where such a presence is indicative of potential illicit or illegal activity." The agency explains that this information is compiled by a third-party provider from multiple commercial sources and anonymized, before being sold to the private sector and government entities including CBP. The agency will retain this data in order to identify patterns, "such as a track that is indicative of a new illegal border crossing trail, or for identification of trends of certain seasonally utilized illegal transit routes."[56]

It is important to note that anonymous location data is not nearly as anonymous as it might appear. In an academic study on the subject, researchers found that individuals could be accurately identified 95% of the time with just four spatio-temporal points of reference.[57]

[55] Byron Tau and Michelle Hackmann, "Federal Agencies Use Cellphone Location Data for Immigration Enforcement," *Wall Street Journal,* February 7, 2020, www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600

[56] DHS, "Privacy Impact Assessment Update for the Border Surveillance Systems (BSS)," August 21, 2018.

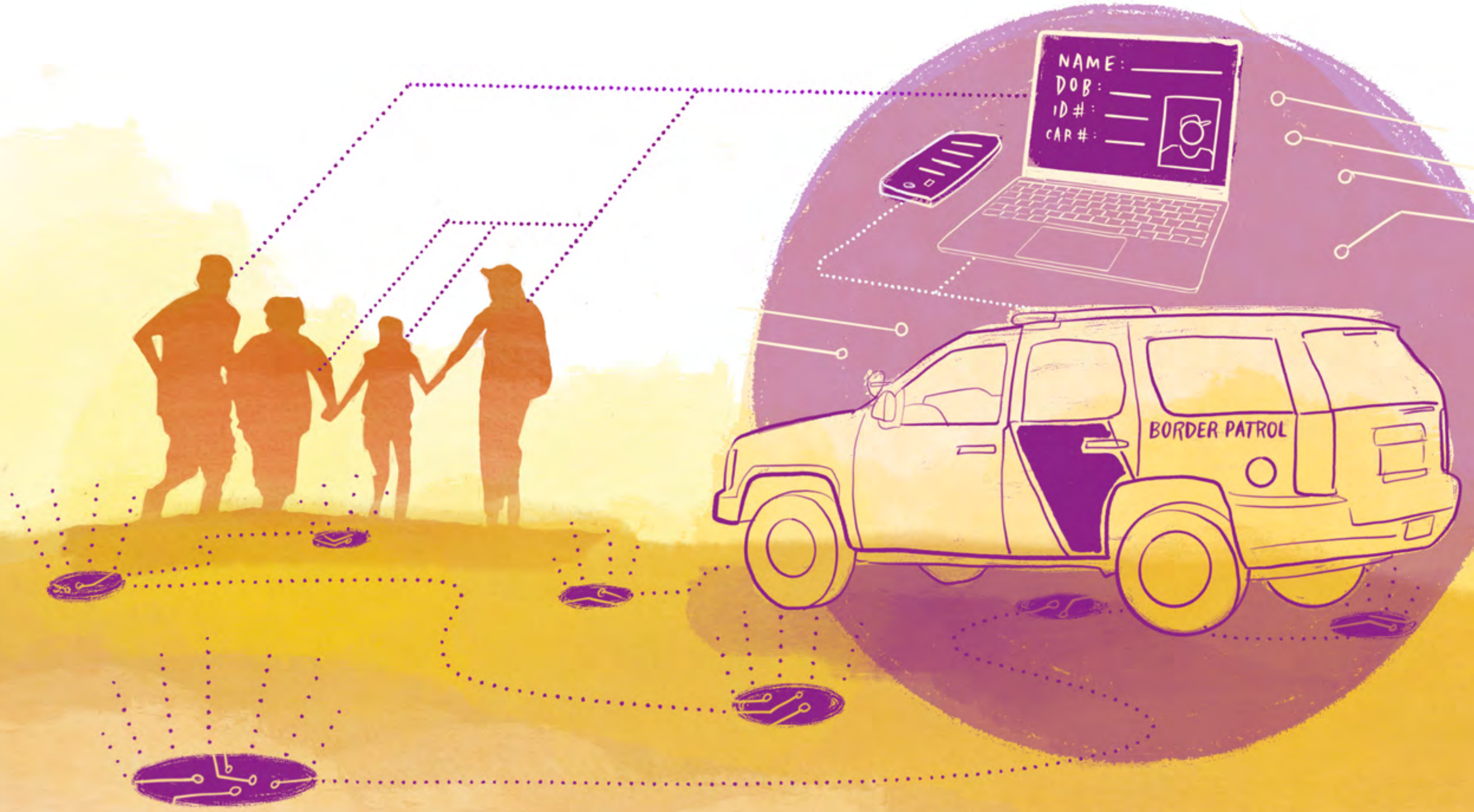
[57] Natasha Lomas, "Researchers spotlight the lie of 'anonymous' data," Tech Crunch, July 24, 2019, https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data.

INTELLIGENT COMPUTER ASSISTED DETECTION

The Intelligent Computer Aided Detection (ICAD) system operates a network of underground sensors and cameras installed along the U.S. border that detects the presence or movement of individuals and relays that information to U.S. Border Patrol. This notifies CBP operators where the alarm occurred, and those operators give direction to agents in the field to respond.[58]

Border Patrol agents input personal details about individuals encountered in the field through ICAD detection, including name, date of birth, document number, license plate number, and other biographic data. The original sensor data is stored by CBP alongside that personal information.[59]

ICAD is used by Border Patrol as its primary system for tracking agent dispatch and for real-time monitoring of unattended ground sensors and other surveillance technology.[60]



[58] DHS, "Privacy Impact Assessment Update for the Border Surveillance Systems (BSS)," August 21, 2018.

[59] DHS, "Privacy Impact Assessment for the Border Surveillance Systems (BSS)," August 29, 2014.

[60] DHS Office of Inspector General, "CBP Has Improved Southwest Border Technology, but Significant Challenges Remain," February 23, 2021, www.oig.dhs.gov/sites/default/files/assets/2021-02/OIG-21-21-Feb21.pdf.

CONCLUSION

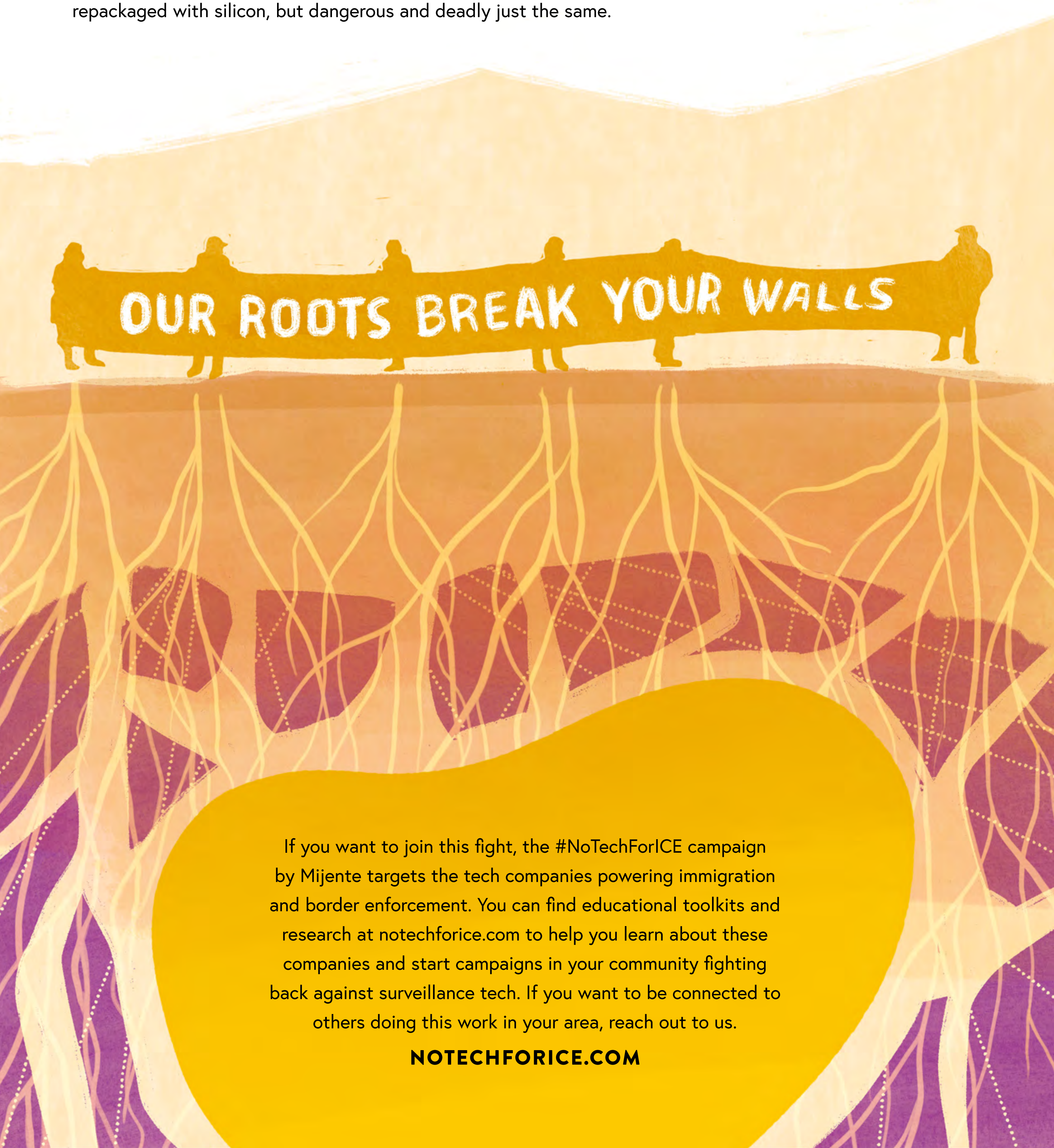
The new border wall is no longer just a concrete and metal barrier, but instead a sprawling network of interconnected systems—drones, surveillance towers, license plate scanners, databases, and more—meant to monitor all aspects of migration and control all activity along the Southwest border. The system as designed is intended to be total: Every person, every car, every animal trekking across the desert would raise an alarm, bringing border patrol agents and leading to more confrontations, more arrests, and more deportations.

Not only that, this digital border wall, despite the bipartisan rhetoric, is deadly. We know border surveillance and increased enforcement pushes people into more remote and more dangerous crossings, leading them through areas where they are more likely to suffer heat stroke, dehydration, and death. This "smart" technology, as Democrats and Republicans alike say, is costing people their lives.

Even those already living in the United States aren't spared. Border communities feel the impact of this surveillance acutely. The surveillance towers above their towns don't just monitor the border, they monitor their backyards too. The drones flying overhead are an ever-present eye in the sky, watching people as they walk, bike, and drive in their neighborhoods. The proliferation of checkpoints is a constant reminder that the entire border region is, in the eyes of DHS, a warzone. Border communities have become a legitimate target for surveillance and enforcement—a taste of what may await the rest of the country as these technologies are rolled out nationwide.

NO BORDER WALL
NO DIGITAL WALL
OPEN BORDERS OPEN HEARTS WE WILL TEAR YOUR WALL APART!
SOMOS FRONTERA NO ZONA GUERRA

We cannot accept this new dystopia. We can and must resist this mass surveillance by exposing the companies and agencies involved, explicitly naming the harm they wreak on migrants and border communities by selling this technology. And we must demand that our lawmakers stop embracing the digital border wall as a "safe" or "smart" alternative. It is the same anti-immigrant logic we saw under Trump, repackaged with silicon, but dangerous and deadly just the same.



If you want to join this fight, the #NoTechForICE campaign by Mijente targets the tech companies powering immigration and border enforcement. You can find educational toolkits and research at notechforice.com to help you learn about these companies and start campaigns in your community fighting back against surveillance tech. If you want to be connected to others doing this work in your area, reach out to us.

NOTECHFORICE.COM