ICE Intelligence Centers: How ICE Gathers Data to Conduct Raids and Deportations

mijente

JUST FUTURES LAW

JAMES H. BINGER CENTER
FOR NEW AMERICANS

UNIVERSITY OF MINNESOTA

ICE Intelligence Centers: How ICE Gathers Data to Conduct Raids and Deportations

Authors

Linus Chan, Allison Maybee, & Marisa Tillman,
University of Minnesota Law School

Julie Mao, Just Futures Law

JUST FUTURES LAW

el Comité mijente

TAKE BACK TECH FELLOWSHIP

Thanks to Empower LLC and David Menninger at the Federal Public Defender Central District of California for their contributions to this report.

A joint publication of Just Futures Law, Mijente, and the James H. Binger Center for New Americans

ICE Intelligence Centers: How ICE Gathers Data to Conduct Raids and Deportations

I. BACKGROUND

As our communities increasingly rely on technologies for communication, employment, and essential services, our data has become the subject of increased surveillance by corporations and governments. For more than a decade, Immigration and Customs Enforcement (ICE) has been building a mass surveillance machine that relies on big data corporations and state-sponsored surveillance to locate, prosecute, and deport individuals. This system of surveillance and criminalization inhibits people's ability to access much-needed health, legal and social services and exercise their right to protest and assemble for fear of being detained and deported. This factsheet sheds light on the rise of one component of this surveillance machine—ICE data surveillance centers (herein "Intelligence Centers")—the cubicles of ICE intelligence analysts who work 24/7 to mine large amounts of data to track down immigrants.

II. OVERVIEW OF ICE INTELLIGENCE CENTERS' DATA TOOLS

ICE has built a massive "cloud industrial complex" to detain, deport, and sometimes prosecute immigrants.[1] ICE has access to the biometric or personal information of millions of individuals, regardless of immigration status, that is collected and stored by the Department of Homeland Security ("DHS"), and other federal government agencies. ICE also has access to information collected by private tech companies such as data obtained via license plate readers and biometric data such as fingerprints, iris scans, and data obtained using facial recognition software. Data collected by state and local governments such as criminal justice or driver's license data are also available to ICE. After collecting this massive amount of information, ICE hires intelligence analysts and tech companies to analyze the massive amounts of data to locate individuals and generate leads for ICE agents to conduct raids.[2]

Major categories of information accessed, bought, and analyzed include:

Local, state, and federal government: Numerous government agencies share data with ICE on individuals. For example, the post office often shares address information with ICE.[3]

Commercial data brokers: Commercial brokers are companies that collect information from numerous sources such as public records, online activity, financial information, credit agencies, cellphone registries, social media, property records, utility accounts, state licenses, and bankruptcy filings. These companies then often sell access to this data to third parties. ICE is a frequent customer. By buying data access from commercial brokers, ICE can bypass some states' restrictions put in place to prevent sharing information directly with ICE.

Data analytics tools: ICE contracts with private companies to analyze vast troves of data and build analytics tools for ICE so that their intelligence analysts can more quickly and easily analyze the data. These data miners are the search engines that help create an "ever-evolving, 360-degree view of U.S. residents' lives."[4]

[1] Mijente et al., *Who's Behind ICE? The Tech and Data Companies Fueling Deportations*, Mijente (2018).

[2] *Id.*

[3] Max Rivlin-Nadler, *How ICE uses social media to surveil and arrest immigrants*, The Intercept (Dec. 22, 2019), ("This data is either openly shared with ICE, as is the case with government agencies like the post office, or collected by data brokers and then sold to ICE. . .")

[4] Department of Homeland Security, *Privacy Impact Assessment for the Data Analysis System* 9 (Sept. 29, 2017).

ICE has not released the names of all of the companies and local, state, or federal agencies from which it obtains data. The following is a sample of the data and analytics tools that ICE intelligence analysts use:

TABLE 1: Example of Data Sources, Data Brokers, and Data Analytics Companies Used by ICE

GOVERNMENT DATA	COMMERCIAL DATA BROKER DATA	DATA ANALYTICS TOOLS
- State driver's license and motor vehicle registration data - State or local criminal justice data - Nlets - FBI's Integrated Automated Fingerprint Identification System (IAFIS)[5] - USCIS Central Index System[6] - ICE EID[7] and IDENT[8] - Postal Service	- LexisNexis[9] - Thomson Reuters[10] - Vigilant License Plate Reader data[11] - APPRISS criminal records - Pen-Link telecommunications data and analytics - Venntel location data and analytics - Giant Oak social media data and analytics - Dun & Bradstreet corporate data	-Palantir -Booz Allen Hamilton -Deloitte

ICE's intelligence centers act as fusion centers. Fusion centers are focal points for the receipt, analysis, gathering, and sharing of information among federal, state, local, tribal, and territorial (SLTT) partners.[12] ICE intelligence centers operate 24 hours a day, 7 days a week. They include a large number of data analytics staff, which has led to it being described as a "cubicle farm." A description of two known intelligence centers follows, but this is just a sample as many different field offices and divisions of ICE may also employ the data analytics tools used at ICE intelligence centers.[13]

PERC official working at the PERC office in Laguna Niguel, California, 2017, photo credit Los Angeles Times.

[5] Department of Homeland Security, *Immigration and Customs Enforcement: Secure Communities Standard Operating Procedure*.

[6] Department of Homeland Security, *supra* note 4, at 7-8.

[7] Department of Homeland Security, *Privacy Impact Assessment Update for the Enforcement Integrated Database (EID) - EAGLE, EDDIE, and DAVID* (May 14, 2019).

[8] *DHS/OBIM/PIA - 001 Automated Biometric Identification System*, Department of Homeland Security (2019).

[9] *Contract Summary: Awarding Agency - Department of Homeland Security, Recipient - LexisNexis Special Services Inc.*, USA Spending (2021), 70CMSD20FC0000054.

[10] *Contract Summary: Awarding Agency - Department of Homeland Security, Recipient - Thomson Reuters Special Services LLC*, USA Spending (2021), 70CMSD18P00000145

[11] U.S. Immigration and Customs Enforcement, *Office of Acquisition Management: ICE Acquisition Manual 3006.301-90* (Mar. 30, 2021).

[12] *National Network of Fusion Centers Fact Sheet*, Department of Homeland Security (Aug. 16, 2019).

[13] *See Law Enforcement Support Center*, U.S. Immigration and Customs Enforcement (Jan. 25, 2021), (explaining that the Law Enforcement Support Center [LESC], considered ICE's "nerve center," is a national law enforcement operations facility also located in Williston, Vermont. LESC is also an ICE intelligence center. The center focuses on conducting immigration status and biometrics checks and sharing the data with state and federal law enforcement agencies. It also helps issue ICE detainer requests to transfer individuals from local custody to ICE. In 2019, it received more than 1.61 million biometric and biographic inquiries from law enforcement agencies seeking information about immigrants.)

National Crime Analysis and Targeting Center (NCATC)

WHAT IS NCATC?

The National Crime Analysis and Targeting Center ("NCATC") is the national enforcement operations center for the ICE Enforcement and Removal Operations ("ERO") Targeting Operations Division, the part of ICE responsible for locating individuals that ICE seeks to detain and deport. Located in Williston, Vermont, NCATC's purported purpose is to apprehend individuals for federal immigration-related offenses such as reentering the U.S. after deportation but has expanded to assist ICE in locating targets for removal.

As ICE explains, NCATC can help locate targets for detention because it *"analyzes large amounts of person-centric data to develop leads"* through "[u]sing technology and partnerships with domestic and international LEAs, interagency stakeholders, and regulatory and intelligence agencies."[14] For example, NCATC uses the Data Analytics System ("DAS"),[15] an analytical database owned and operated by ERO. It contains various datasets, including biographical information, criminal history and databases, immigration history, commercial data broker data, multiple federal agency data, and vehicle and insurance information, among others. **In Fiscal Year 2019 alone, NCATC surveilled and analyzed 5.1 million individuals for targeting information and disseminated thousands of leads to ICE field offices and divisions to conduct raids and detentions.**[16]

HOW IT WORKS:[17]

- ICE would develop a target and send data on those targets that it seeks to deport to NCATC to run through its database to develop leads on their best-known address or location. DHS's other agencies may also send leads to NCATC as well. For example, in *U.S. v. Valadez-Munoz*, it was the United States Citizenship and Immigration Services ("USCIS") and not ICE that sent data about an individual to NCATC.

- NCATC pulls data from federal or local agencies, public records, and commercial data brokers to match the name, photo, and other identifying information from the data sources and platforms accessible to ICE. *See* Table 1.[18] NCATC analysts will review government and commercial databases and platforms such as motor vehicle car registrations, utility bills, USPS mailing addresses, and other records. For example, in *U.S. v. Valadez-Munoz*, an NCATC official conducted searches of databases to track down the individual, successfully obtaining a home address on a driver's license via access to Nlets which led to his arrest for reentry after deportation.

- After analysis, NCATC will then send information to ICE field officers to locate the targets for detention, prosecution, and deportation.

[14] Department of Homeland Security, *U.S. Immigration and Customs Enforcement budget overview: Fiscal year 2021 congressional justification* 150 (2021).

[15] Department of Homeland Security, *supra* note 4.

[16] U.S. Immigration and Customs Enforcement, *Enforcement and Removal Operations* (May 11, 2020).

[17] Rivlin-Nadler, *supra* note 3.

[18] Cora Currier, *Lawyers and Scholars to LexisNexis, Thomson Reuters: Stop Helping ICE Deport People*, The Intercept (Nov. 14, 2019), (explaining NCATC contracts with many private vendors, but most are unknown and not public information. Two that are known are contracts with Thomson Reuters CLEAR and LexisNexis).

NCATC CASE STUDIES		
STATE	IMMIGRANT'S ACTIONS	NCATC/ICE INVOLVEMENT
New Mexico[19]	The individual renewed his New Mexico driver's license, which listed his address. This state motor vehicle data was accessible to ICE through NCATC.	ICE received a referral from the NCATC. NCATC matched the individual's driver's license photo to his photo and fingerprints from a prior arrest. Federal immigration authorities filed an arrest warrant and arrested him within a year.
Florida[20]	The individual applied for worker's compensation with the state of Florida, which included submitting his address. The worker's compensation database was accessible to ICE through NCATC.	NCATC sent his address (the one he submitted for his worker's compensation application) to ICE. ICE ERO officers were then sent to his home, encountered him, and detained him.

Pacific Enforcement Response Center (PERC)

WHAT IS PERC?

The Pacific Enforcement Response Center ("PERC") is an ICE office composed of analysts that supplement the work of ICE field offices by providing intelligence support, searching databases and other sources to track down immigrants, and placing detainers on immigrants in custody across the U.S. Often, ICE field offices will contact PERC to investigate specific cases.[21] The PERC office is located in Laguna Niguel, California. Like NCATC, ICE uses data that PERC collects against all persons who may be eligible for deportation as a dragnet surveillance tool.

PERC analysts have access to a wide range of databases and data analytics tools. Specifically, PERC analysts use these tools to {1} search for information relating to cases in which ICE field officers request PERC support, including searching the targeted individual's social media, searching for the individual's (or their family's) address(es), place(s) of work, driver's license(s), or other identifying information that would allow ICE to track the individual and arrest them, and {2} issue ICE detainers and notifications to local jails and prisons across the country so ICE can pick up people at the time of their release from those facilities. PERC issues about 40% of all immigration detainers and requests for notification when jails release individuals.[22]

HOW IT WORKS:

ICE field offices contact PERC for help in tracking down the location of an individual that ICE has targeted.

- PERC officials use various databases, including commercial databases, at their disposal to search for information on the individual, including address, workplace, friends' and family's information, etc. PERC officials use other tools like social media to gain more information.

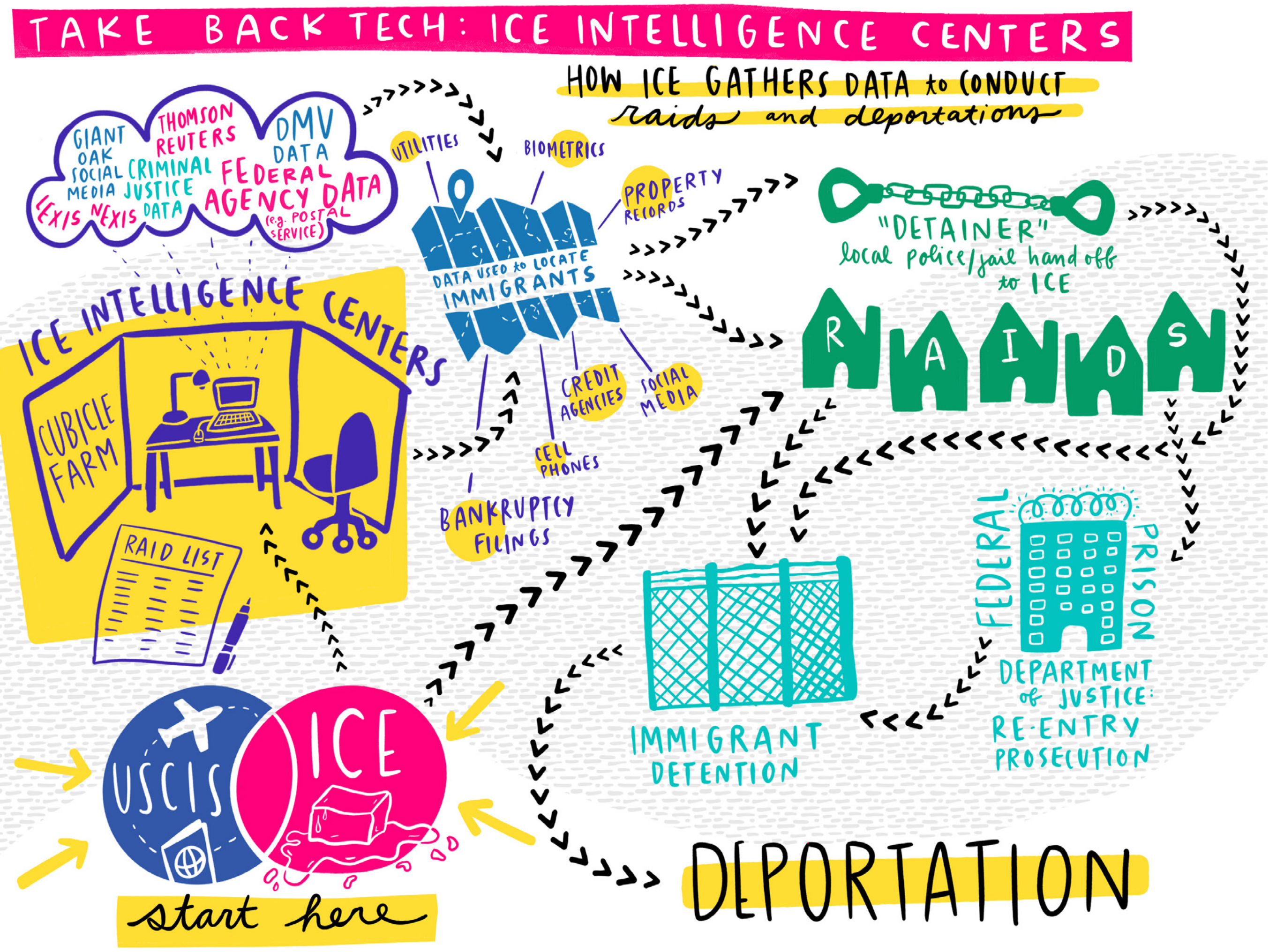
[19] *U.S. v. Olivas-Perea*, 297 F. Supp. 3d 1191 (D.N.M. 2017) (No. CR 16-4518 JB) (memorandum opinion and order).
[20] Criminal Complaint, *U.S. v. Diaz-Antunez*, No. 8:17-cr-00057-CEH-MAP (M.D. Fla. Jan. 24, 2017).
[21] Amy Taxin, *Immigration detainers often issued by California center*, The Orange County Register (Sept. 20, 2015); Rivlin-Nadler, *supra* note 3.
[22] Taxin, *supra* note 22.

- PERC officials send these intelligence leads to ICE field offices. To issue a detainer, PERC first receives electronic notifications based on biometric information taken by law enforcement officials when an individual is booked into law enforcement custody.

- When fingerprints are taken during booking, they are sent to the FBI CJIS Integrated Automated Fingerprint Identification System ("IAFIS") system. IAFIS automatically sends the fingerprints onto the ICE Automated Biometric Identification System ("IDENT"), which searches for matches to fingerprints already in the DHS System. If there is a match, the information flows to ICE's Law Enforcement Support Center ("LESC"), which searches multiple databases to compile information on individuals.

- This information then goes to PERC. PERC then lodges a DHS immigration detainer with local law enforcement on the same day.[23]

ICE INTELLIGENCE CENTERS VISUAL GRAPHIC



[23] Criminal Complaint, *U.S. v. Garcia*, No. CR-00454-PSG (C.D. Cal. July 24, 2019); Findings of Fact and Conclusions of Law, *Gonzalez v. ICE*, 416 F. Supp. 995 (C.D. Cal. 2019) (No. 2:12-cv-09012-AB).

PERC CASE STUDIES		
STATE	IMMIGRANT'S ACTIONS	PERC/ICE INVOLVEMENT
Indiana[24]	Local police arrested the individual, and they were in the custody of the Dubois County Sheriff's Department, Jasper, Indiana.	PERC received an electronic notification based on biometric fingerprint information that he was in custody that same day. PERC then lodged a DHS Immigration Detainer immediately.
California[25]	The individual worked as a roofer and would regularly post on Facebook. On May 24, 2018, he "checked in" on Facebook at Home Depot to buy roofing supplies. He was then stopped and arrested by ICE officers as he left the parking lot.	On February 22, 2018, the Los Angeles ICE field office received a lead from NCATC on the individual. The Los Angeles ICE office contacted PERC for help tracking him. A PERC official found the individual's Facebook account. The PERC official also used Thomson Reuters CLEAR database to find his address. PERC cross-referenced this address with photos on the individual's Facebook to confirm the Facebook page belonged to him. ICE officers began monitoring his Facebook page. When the individual "checked in" on Facebook at a Home Depot, ICE officers went to the Home Depot and arrested him.

Why Are ICE Intelligence Centers Concerning?

While ICE has used surveillance tactics for decades, the expansion of ICE intelligence centers—where throngs of intelligence officers work 24/7 analyzing surveillance databases from local, federal, and corporate entities to track down millions of people—represents a dangerous new frontier in mass surveillance. Below, we highlight a number of reasons why ICE Intelligence Centers are deeply troubling and should be shut down.

Increased Mass Deportation and Criminalization: The mission of these ICE Intelligence Centers is to conduct mass surveillance on millions of individuals for ICE to detain and deport immigrants. This surveillance will lead to more raids, more ICE agents, more deportation, and more families and communities separated.[26] As the above case examples highlight, these Centers also lead to the increased prosecution and imprisonment of individuals for the federal offense of reentering after deportation. This type of mass surveillance is not possible without collecting information on everybody, citizen or not. Vastly expanding the surveillance state threatens every community's right to privacy and freedom.

Expand and Perpetuate Racial Profiling and Bias: Black, indigenous, and people of color communities are hyper-policed with technologies and entangled within the criminal legal system. ICE surveillance programs heavily rely on police action, data, and surveillance technologies embedded with racial bias, and thereby perpetuate the racist history of policing and prisons in the U.S. Moreover, the laws used to prosecute people for reentering the U.S. after deportation are rooted in racism, eugenics, and white supremacist ideology[27] and continue to have a starkly discriminatory impact on Black and Brown communities.

[24] Criminal Complaint, *U.S. v. Quijada-Velasquez*, No. 3:18-cr-00030-RLY-MPB (S.D. Fla. Apr. 25, 2018).

[25] Rivlin-Nadler, *supra* note 3.

[26] *ICEwatch: ICE Raids Tactics Map, A Brief Summary of ICE Raids Trends to Accompany*, Immigrant Defense Project, Center for Constitutional Rights (July 2018).

[27] See Kelly Lytle Hernández, City of Inmates: Conquest, rebellion, and the rise of human caging in Los Angeles, 1771–1965 137 (UNC Press Books, 2017). *See also* Madlin Mekelburg, *Fact-check: When did it become a crime to cross the U.S. border between ports of entry?*, Statesman, July 12, 2019.

Chilling Impact on Immigrants: Mass surveillance and data tracking hinder access to essential services such as utilities, driver's licenses, cell phones, and internet for everyone, particularly immigrants, for fear of criminalization and deportation.

Erosion of the Fourth Amendment and Local Policies Limiting ICE Collaboration: The Fourth Amendment's prohibition on unreasonable search and seizures protects government surveillance of personal location data. Additionally, many local jurisdictions have policies limiting data sharing and collection with ICE. However, DHS circumvents these protections by purchasing data from commercial data brokers and corporations, which extract the data from consumers and local agencies.[28]

Unreliability of Databases: Programs like PERC and NCATC often contain incomplete data, significant errors, or were not designed to determine a person's removability, leading to ICE using this information to make erroneous arrests.[29] For example, between May 2015 and February 2016, 771 of 12,797 (6%) requests that ICE issued were either for U.S. citizens or people who were not subject to deportation, according to records introduced at trial last year.[30]

What Can You Do?

We must intervene in the tech-driven deportation machine that ICE and DHS are deploying against immigrant, Black, and Brown communities. The parade of increasingly invasive technologies makes clear that ICE is working in collaboration with tech companies and governments to build a massive surveillance apparatus to track and criminalize all. There are many ways to challenge ICE's mass surveillance programs through advocacy, litigation, education, research, and organizing. We highlight some below:

Local Government Accountability: Much of ICE and DHS data comes from data sharing between federal and local government agencies. State and local government agencies should be held accountable for what technologies they use and how they share their data. Local jurisdictions should limit funding and the use of mass surveillance technologies and data sharing.

Tech Corporate Accountability: The increasing collaboration between DHS and private tech companies, such as data brokers, fuels a system in which corporations profit from surveillance products. This is a clear example of how "surveillance capitalism" works in the service of criminalization.[31] As consumers and advocates, we should demand greater accountability from corporations that sell our data and contract with DHS to facilitate mass detention and deportation.

DHS and Federal Government Accountability: We do not know where ICE gets all of its information. Some of these contracts have been kept from the public. We must advocate for transparency in how ICE gets personal information and data for individuals to hold them accountable to the public. We must also demand that Congress limit funding to DHS for tech surveillance, detention, and deportation.

[28] *See e.g.* Letter from Sherrod Brown,U.S. Sen., Edward J. Markey, U.S. Sen., Brian Schatz, U.S. Sen., Elizabeth Warren, U.S. Sen, & Ron Wyden, U.S. Sen., to Joseph V. Cuffari, Inspector Gen., Dep't of Homeland Security (Oct. 23, 2020), (requesting Mr. Cuffari investigate the warrantless surveillance of phones through commercial databases by Customs and Border Protection).

[29] *Id.*

[30] *Id.*; Elliot Spagat, *Judge strikes blow to U.S. immigration enforcement tactics*, Associated Press (Feb. 7, 2020), ("In a Federal Judge ruling in the Central District of California, Judge Andre Birotte, Jr. wrote, '...the databases are unreliable for people who are not already deported or in removal proceedings before an immigration judge.'")

[31] *Technology & Criminalization*, Astraea Lesbian Foundation for Justice, Technologies for Liberation, Research Action Design (2020).