# DHS's Data Reservoir



## ICE and CBP's Capture and Circulation of Location Information

epic.org

August 2022

## ABOUT THE AUTHOR

Dana Khabbaz is the 2021-2022 Justine Wise Polier Fellow at the Electronic Privacy Information Center (EPIC). As part of the Project on Surveillance Oversight, Dana's advocacy counters the unchecked expansion of government surveillance, with a particular focus on location surveillance in immigration enforcement. At EPIC, Dana's advocacy has included contributions to FOIA litigation, amicus briefs, policy advocacy, and administrative comments. Dana is a graduate of Yale Law School and Indiana University.

## ABOUT THE ELECTRONIC PRIVACY INFORMATION CENTER

The Electronic Privacy Information Center (EPIC) is an independent, nonprofit organization that has been focusing public attention on emerging privacy and civil liberties issues since 1994. Through its Project on Surveillance Oversight, EPIC advocates for greater oversight of surveillance systems and closely tracks domestic surveillance issues to ensure that civil liberties are protected.

## ACKNOWLEDGEMENTS

The author would like to thank EPIC's Director of the Project on Surveillance Oversight, Jeramie Scott, for his expertise, guidance on shaping this report, and review of this report; EPIC Law Fellow Jake Wiener for his reviews, analysis, design support, and advice; EPIC Senior Counsel Megan Iorio for her advice on shaping this report; Melodi Dincer for providing contextual research; and the EPIC staff for their review of this report. Finally, the author would like to thank the Yale Law Journal for their funding and support of this fellowship. The views expressed in this report are those of EPIC and the author.

# TABLE OF CONTENTS

# ACRONYM GUIDE

**AFI** – CBP Analytical Framework for Intelligence

**CBP** – U.S. Customs and Border Protection

**CLEAR** – a data mining and analysis program sold by Thomson Reuters

**DAS** – ICE Data Analysis System

**DHS** – Department of Homeland Security

**DMV** – Department of Motor Vehicles

**ELSUR** – Electronic Surveillance System

**EID** – Enforcement Integrated Database

**ERO** – Enforcement and Removal Operations (subdivision of ICE)

**FALCON – SA** – FALCON Search & Analysis System

**FBI** – Federal Bureau of Investigation

**GPS** – Global Positioning System

**HSI** – Homeland Security Investigations (division of Immigration and Customs Enforcement)

**ICEPIC** – ICE Pattern Analysis and Information Collection

**ICM** – ICE Investigative Case Management

**IFS** – Intelligence Fusion System

**IIRS** – ICE Intelligence Records System

**IMSI catcher** – another name for a cell-site simulator or Stingray

**LPR** – license plate reader

**NCATC** – National Criminal Analysis & Targeting Center (subdivision of Immigration and Customs Enforcement)

**NCTUE** – National Consumer Telecom & Utilities Exchange

**PAIG** – Publicly Available Information Group

**PIA** – Privacy Impact Assessment

**PII** – personally identifiable information. Information that could be used to identify a person

**SORN** – System of Records Notice

**TECS** – Not an acronym. A Customs and Border Protection records system.

**TSA** – Transportation Security Administration

**USCIS** – U.S. Citizenship and Immigration Services (a component of DHS)

**USPS** – United States Postal Service

# INTRODUCTION

Recent technological advancements have made previously unfathomable quantities of personal data accessible with unprecedented ease to federal law enforcement agencies, including the Department of Homeland Security ("DHS") sub-agencies Immigration and Customs Enforcement ("ICE") and Customs and Border Enforcement (''CBP"). Location information is one of the most revealing and invasive types of information DHS collects. In the hands of immigration enforcement agencies, it is a tool to monitor, track down, detain, and deport immigrants. The location information in ICE and CBP's arsenal includes precise geolocation obtained from digital devices like cell phones. It also includes more general location information that can be deduced from data like home, work, and school addresses; vehicle license plates detectable by license plate readers countrywide; and even information about the people with whom an individual associates.

Location information travels through a complex network of ICE and CBP subcomponents and records systems. It often begins with the agencies' use of surveillance technologies that directly capture location information or with the agencies purchasing location information from commercial data brokers. From there, the information frequently exchanges hands—spreading within and among ICE and CBP's numerous and overlapping internal databases.

For years, privacy rights and immigrant justice advocates have been sounding the alarm on ICE and CBP's indiscriminate access to sensitive personal information about immigrants, travelers, and immigrant communities.[1] Meanwhile, ICE and CBP continue expanding their information collection operations, gradually forgoing traditional methods of surveillance in favor of bulk purchases and transfers of personal information from commercial data brokers and from other federal, state, and local agencies. As the agencies have steadily adopted new and more indirect methods of obtaining and disseminating location data, they have managed to sidestep traditional privacy protections afforded by the Fourth Amendment and privacy laws. Affected immigrants are left with little control or transparency regarding the circulation of their personal information and the use of that information to enable their deportations, arrests, and confinement.

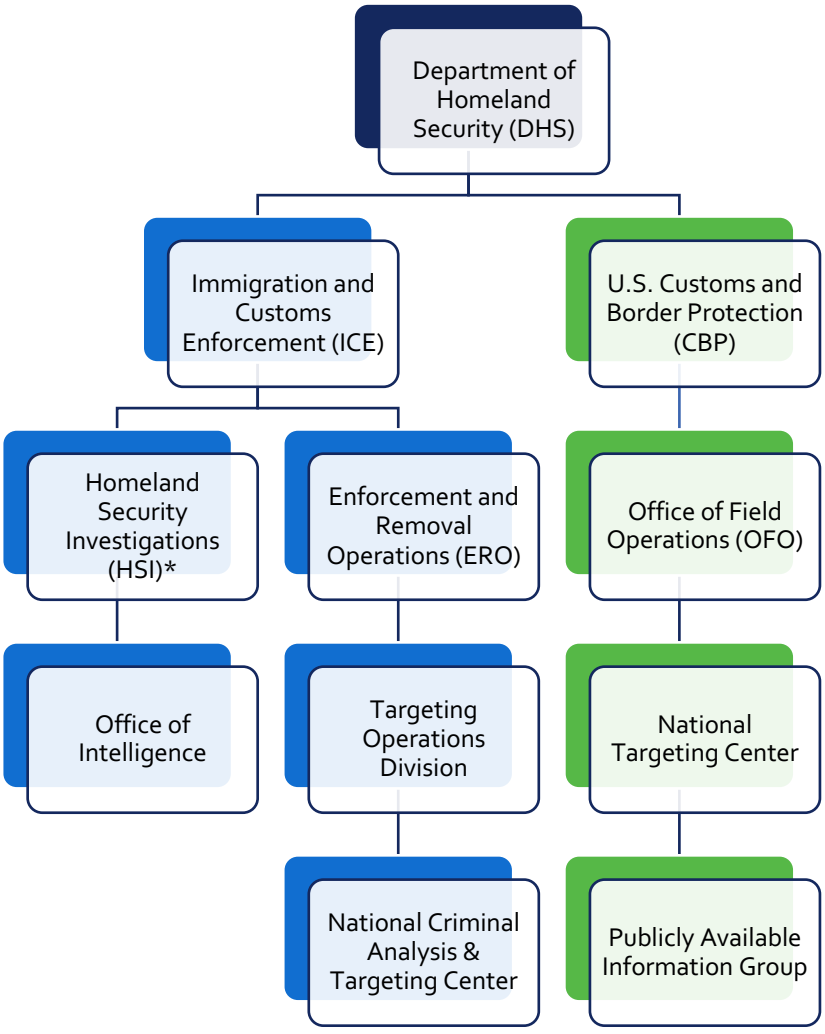
This report provides a guide to some of ICE and CBP's key methods used to obtain location information, as well as some of the major databases in which the agencies store location information. This report provides a sketch of the systems that operate behind the scenes to collect and disseminate sensitive information about immigrants, travelers, and immigrant communities. A complete understanding of how these systems operate remains elusive, however—until DHS grants the public more transparency regarding into the technology the

agency uses, the information it accesses and disseminates, and the privacy measures it implements.

Part 1 of this report provides an overview of types of location surveillance technologies and methods of obtaining location information utilized by ICE and CBP. Part 2 describes some of the ICE and CBP databases and records systems that store location information. Finally, Part 3 provides the following policy recommendations: (1) that DHS end purchases from commercial data brokers and require a warrant before accessing sensitive location data; (2) that DHS end bulk collection and transfers of location data, and end use of sensitive data for development of new leads; (3) that DHS should limit storage times for sensitive data; (4) that DHS disclose commercial databases that it accesses but does not store internally; (5) for DHS to consider precise location information to be "personally identifiable information" and comply with the Privacy Impact Assessment requirement of the E-Government Act; and (6) for DHS to end surveillance as an "alternative" to other methods of control.

# OVERVIEW OF RELEVANT DHS SUB-COMPONENTS

This guide discusses the use of location data by two sub-components of the Department of Homeland Security: Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP). This guide also references several key divisions and groups under ICE and CBP that use location information. Below is diagram of the hierarchical relation between ICE/CBP and their relevant divisions and groups.




*Of particular interest to this report is HSI's National Tracking Program, which manages location-tracking technologies.

# OVERVIEW: HOW LOCATION INFORMATION TRAVELS

## Home Address

**Collected via:**
- Utility bills
- Property records
- Credit reports
- Publicly available information
- State DMVs
- USPS

**Stored In:**
- CBP AFI
- CBP TECS
- ELSUR
- FALCON-SA
- ICE DAS
- ICE EIS
- ICE ICM
- ICE PIC
- IFS
- Possibly ICE IRS

## License Plates

**Collected via:**
- Gov't LPRs
- Commercial LPR databases
- State DMVs

**Stored In:**
- CBP AFI
- CBP TECS
- FALCON-SA
- ICE DAS
- ICE EIS
- ICE ICM
- Possibly ICE PIC

## Digital Device Location

**Collected via:**
*Includes cell phone, ankle monitors, smart devices*
- Gov't cell-site simulators
- GPS trackers
- Data brokers

**Stored In:**
- ELSUR
- FALCON-SA
- ICE EIS
- ICE ICM
- Possibly CBP AFI
- Precise mobile location data from data brokers is not usually stored in DHS systems.

## Other Location Data

**Collected via:**
*includes addresses, personal relationships*
- Social media
- Publicly available information
- Property records
- Legal records
- Credit reports

**Stored In:**
- FALCON-SA
- ICE DAS
- ICE ICM
- ICE PIC
- IFS
- Possibly CBP AFI
- Possibly ICE EIS

# TYPES OF LOCATION SURVEILLANCE & LOCATION DATA COLLECTION

ICE and CBP collect large quantities of personal data on American citizens, immigrants, travelers, and others. Much of that data can be used to reveal individuals' locations. "Location information" as defined in this report includes precise location information at a specific date and time—such as GPS coordinates—and more persistent location information—such as a person's home or work address.

ICE and CBP use three overarching methods to accumulate location information: (1) by direct surveillance using their own surveillance technologies, (2) by purchasing data from commercial data brokers, or (3) by receiving the data from other government agencies that themselves employ methods (1) or (2). Below is a description of five sources ICE and CBP use to obtain location information: cell-site simulators, mobile application location data aggregators, GPS data through direct surveillance and commercial data brokers, profile information from data brokers, and license plate reader data.

## CELL-SITE SIMULATORS

**WHAT THEY ARE:** Cell-site simulators are devices that mimic cell-site towers.[2] Cell-site towers are towers mounted with antennas and other equipment that produce a cellular signal. When cell phones connect to cell-site towers, the phones transmit data to the towers. That transmission can reveal the approximate location of a cell phone. Location data from cell-site towers is less precise than GPS location data.[3]

Cell-site simulators (also known as Stingrays or IMSI catchers) mimic cell-site towers, tricking nearby cell phones into connecting with them and transmitting data. Through this connection, cell-site simulators can obtain a time stamp, location radius, and signal strength from the connecting phone. This data can reveal the approximate location of the cell phone at a particular time. Cell-site simulators are often used by law enforcement agencies to capture phone location information.[4]

**WHICH AGENCIES USE THEM:** ICE[5] and CBP.[6]

**DIRECT SURVEILLANCE OR DATA PURCHASES:** Direct surveillance.

**COMPANIES THAT ARE SELLING THEM TO DHS:** L3harris, possibly others.

**WHAT WE KNOW ABOUT HOW DHS AGENCIES ARE USING THEM:** Since 2018, the government has been required to obtain a warrant before obtaining cell-site location information. In 2018, the Supreme Court's decision in *Carpenter v. United States* held that individuals have a reasonable expectation of privacy with respect to their historical cell site location information, ending the government's ability to search cell-site location information without a warrant.[7] It is unclear to what extent ICE and CBP still rely on cell-site simulators, as compared to other methods, for their location data collection.

ICE Homeland Security Investigations (HSI) uses cell-site location information for their criminal investigations. Agents are required to obtain a search warrant prior to using cell-site simulators. HSI uses cell-site simulators in two ways: for "target location" and for "target development." When using it for "target location," agents target their search only to a specific mobile identifier and obtain location information for that mobile device only. When using the cell-site simulators for "target development," agents collect the location data of all phones captured by a simulator. After completing that search and capturing that data, the agents will determine which mobile devices should be the "target devices."[8]

**HOW DATA IS STORED:** In HSI investigations, data from non-target devices is deleted within 24 hours of a cell-site simulator search.[9] Data from target devices is stored for longer periods of time within DHS systems.

## MOBILE APPLICATION LOCATION DATA AGGREGATORS

**WHAT THEY ARE:** Mobile application location data is location data collected from smartphone applications. Ordinary mobile applications on smartphones—including apps for "games, weather and e-commerce" regularly collect users' location data.[10] Unbeknownst to the average smartphone user, location data from these everyday applications is packaged by data aggregators and sold by data brokers to government and commercial buyers.[11]

Location data from smartphone applications is precise and includes latitude-longitude coordinates. The location coordinates in this data can come from "GPS signals, cell tower triangulation, WiFi data, or by other techniques."[12] Location data from smartphone applications is linked to specific devices through an "ad-ID." Ad-IDs are unique identification codes for digital devices, and they are ordinarily used in the advertising industry.[13] Data brokers like Venntel and Babel Street sell access to this location data in bulk.

**WHICH AGENCIES USE THEM:** CBP (particularly through its National Targeting Center's Publicly Available Information Group),[14] ICE (both ERO and HSI).

**DIRECT SURVEILLANCE OR DATA PURCHASES**: Data purchases.

**WHAT COMPANIES ARE SELLING THEM:** Venntel, Babel Street, Gravy Analytics.

**WHAT WE KNOW ABOUT HOW DHS AGENCIES ARE USING THEM:** Venntel and Babel Street sell access to web-based applications to ICE and CBP. Through these applications, a subset of authorized ICE and CBP agents can search databases of location information.[15] The location information is anonymized—agents can only see an "Anonymized Record ID," which is an anonymized version of an ad-ID. The ad-IDs of devices are known only by the data vendor. DHS agencies have to issue a subpoena to acquire the identity of an anonymized record ID.[16]

ICE and CBP consider anonymized record IDs not to be "personally identifiable information" (PII).[17] PII is a privacy term for information that can an identify a person, and data that has PII requires heightened privacy measures. As numerous studies have shown, however, precise mobile location data is not truly anonymous.[18] One study published in 2022 even demonstrated that "anonymized" mobile location data could be de-anonymized up to 85% of the time.[19] Thus, despite ICE and CBP's assertions otherwise, the anonymized location information accessible through these mobile

location applications can be used to identify a person and therefore do meet the definition of "personally identifiable information."

Moreover, Gravy Analytics, Venntel, and Babel Street sell not only access to location data, but also access to a software that analyzes that data for patterns over "a period of days, weeks, or months"—including a device's "frequented locations" and other devices it associates with.[20] The software also allows CBP and ICE agents to filter devices by date, time, and location.[21] The data brokers sell access to a massive amount of data—Gravy Analytics, for example, boasts access to "15+ billion daily location signals from 250 million mobile devices."[22]

ICE HSI uses mobile application location data for its criminal investigations—domestic and international.[23]

**HOW DHS STORES THE DATA:** DHS does not store data from mobile application location data brokers. The software DHS accesses are web-based only.

## OTHER GPS DATA

**WHAT THEY ARE:** GPS data is precise location data derived from satellite signals. GPS data can be collected from GPS tracking devices, as well as digital devices including cell phones. Below is a description of DHS use of GPS data from sources other than vendors that aggregate mobile location data.

**WHICH AGENCIES USE THEM:** ICE and CBP.

**DIRECT SURVEILLANCE OR DATA PURCHASES:** Direct surveillance, and some data purchases.

**WHAT COMPANIES ARE SELLING THEM:** CovertTrack, Caron East Inc., Venntel, Babel Street, Sendum Wireless Corporation,[24] Motorola Solutions Inc.,[25] Communications Engineering,[26] Special Services Group,[27] Coleman Technologies Inc.,[28] Orion,[29] Cobham Tracking & Locating,[30] GPS Intelligence,[31] Ensurity Mobile Corp.,[32] Starchase LLC,[33] and Freightwatch International.[34]

**HOW ICE AND/OR CBP ARE USING THEM:** Within ICE HSI, the National Tracking Program manages location-tracking technologies, including the use of GPS tracking. HSI policy requires a warrant before using a GPS tracking device, with limited exceptions. ICE HSI often discloses location data information generated by GPS tracking devices with other law enforcement agencies.[35]

HSI agents have access to a web-based application that allows them to view location tracking devices on "real-time maps." It is not clear whether this application is through Venntel or Babel Street or a similar vendor. Through another internal application, ICE HSI can also generate maps that show real-time movements of GPS trackers. ICE HSI can link a GPS tracking device to an individual person by "manually inputting the data" into the ICE HSI case management tool, Investigative Case Management (ICM).[36]

ICE also uses GPS location tracking in its "Alternatives to Detention" program. The Alternatives to Detention program purports to serve as a more humane alternative to immigration detention, but the program has been a vehicle through which DHS has ramped up surveillance and data collection. What's more, the program has been used on immigrants who would not otherwise have been subject to detention.[37] The Alternatives to Detention program employs several methods to monitor immigrants' locations, including using GPS ankle monitors and using a mobile application called SmartLINK.[38] Immigrants use the the SmartLINK application to monitor asylum seekers and immigrants facing deportation and to facilitate communication about their cases. Location

information is collected by the application during "check-ins," but immigrants must provide the application permission to track their location at all times.[39] Commercial data brokers that aggregate mobile location data are also collecting GPS data from ankle monitors used in ICE's Alternatives to Detention program.[40] It is not clear whether DHS has imposed any restrictions on these data brokers to prevent them from then reselling ankle monitor location data to other commercial data brokers or to other government agencies.

Further, GPS location data is collected in CBP's new mobile application, CBP One. Users of the CBP One app can access CBP services through the app. For example, CBP One users can use the app to fill out and pay for arrival/departure forms or self-report their exits from the United States at certain parts of the border.[41] When CBP One app users report to the app that they are entering or exiting the United States, the application pings their cell phones to obtain their GPS coordinates and sends those coordinates to CBP.[42]

**HOW DATA IS STORED:** GPS data obtained indirectly through data brokers like Venntel and Babel Street are not stored in DHS systems. Venntel and Babel Street sell access to exclusively web-based software applications.[43]

Spreadsheets with location-tracking information may be uploaded by ICE into ICE's Investigative Case Management tool, and those spreadsheets may contain device identifiers.[44] ICM stores its records for 20 years.[45]

The GPS coordinates collected through the CBP one app are not visible to CBP officers and agents. CBP stores the information in separate systems—it does not store the information locally on the application or in the user's cell phone.[46]

## LICENSE PLATE READERS

**WHAT THEY ARE:** License Plate Readers (LPRs) are cameras that can scan license plates, capturing the license plate number, GPS coordinates, information about the vehicle's make and model, and time stamp. Sometimes, LPRs can capture images of individuals in a vehicle. LPRs are often placed on street poles, police cars, and highway overpasses.[47]

**DIRECT SURVEILLANCE OR DATA PURCHASES:** Both. LPR cameras capture primary data—images and time stamps for license plates in their vicinity. Software integrated with those cameras can cross-reference the captured data with secondary data—existing databases with license plate information and other data. CBP also purchases license plate reader information from private vendors which, in turn, collect the data from commercial license plate readers nationwide.

**WHICH AGENCIES USE THEM:** Both ICE and CBP use LPRs.

**COMPANIES THAT ARE SELLING THEM TO DHS:** NDI Technologies,[48] Motorola Solutions (Vigilante),[49] Thomson Reuters,[50] Leonardo DRS (Selex Es),[51] RTR Technologies,[52] LA Tech,[53] LexisNexis (Accurint).[54]

**HOW ICE AND/OR CBP ARE USING THEM:** CBP collects license plate information in three ways: (1) through identifiable LPRs attached to vehicles, (2) through hidden LPRs attached to fixed structures, and (3) indirectly by purchasing the license plate data from vendors that amass information from LPRs nationwide.

CBP's mobile LPRs are attached to CBP vehicles. CBP's covert LPRs are positioned on fixed structures near roadways and are unmanned.[55] In addition to these primary data collection methods, CBP also purchases license plate information from commercial vendors. These vendors "collect license plate information from private businesses (e.g., parking garages), local governments (e.g., toll booth cameras), law enforcement agencies, and financial institutions via their contracted repossession companies."[56]

CBP's commercial license plate vendors collect license plate information from readers nationwide—including regions outside CBP's "border zone" jurisdiction, but the readers do not collect information from outside the United States.[57] CBP doesn't use commercial license plate information to generate new leads. Agents can only access license plate information of people who CBP has separately identified as "believed to be involved in illegal activity in connection with CBP's law enforcement or border security mission."[58]

ICE both uses its own LPRs and obtains LPR data.[59] Using LPR databases of other federal, state, and local law enforcement agencies, ICE can obtain real-time location information from LPRs that are attached to law enforcement vehicles nationwide.[60] ICE has a "hot list" of license plates, and ICE agents can receive notifications when license plates on that list are captured by a government LPR. The notifications include "GPS coordinates for the location where the license plate was photographed."[61]

Separately, ICE has also been purchasing access to commercial license plate reader databases since 2015 for use by its Enforcement and Removal Operations (ERO) and Homeland Security Investigations (HSI) arms.[62] ICE users can search these license plate databases by searching a full or partial license plate number; the vehicle's make, color, model, and year; or by geographic area.[63] The ability to search by geographic area and vehicle type is available only to HSI criminal investigations and is not available to ICE's enforcement and removal operations. HSI users can also analyze "pattern of vehicle movement"—detailed information about where a vehicle has traveled, including driving to work, school, or the doctor.[64]

HSI users are not required to obtain a warrant before conducting these database searches—all that is required is "reasonable suspicion that the queried area is associated/linked to an ongoing investigation."[65] Notably, the use of "reasonable suspicion" here is different from how the term is commonly used in other criminal contexts, where the standard is a reasonable suspicion that a person is engaging in or about to engage in the commission of a crime.

ICE and CBP share license plate data with each other and have data-sharing agreements with other federal, state, and local agencies, including local law enforcement agencies.[66]

**HOW DATA IS STORED:** ICE ERO stores hard copy LPR records for three years (unless "there is a justified business need" to store the records longer). Any information related to LPRs that ICE ERO inputs into its enforcement database is electronically stored in that database for 75 years. ICE HSI stores hard copy LPR records for 10 years onsite and 20 years at the Federal Records Center (with limited exceptions that can justify longer storage). These limits do not apply to commercial vendors, who may store their LPR data indefinitely.[67]

CBP retains "up to five years of historical data" in its databases of LPR information.[68]

## PROFILE INFORMATION

**WHAT THEY ARE:** In addition to license plate databases and mobile application location data, data brokers also sell other data—information that can allow immigration enforcement agencies and other law enforcement to create comprehensive profiles of their targets. Unlike mobile application data brokers like Venntel, these data brokers do not sell precise-location-focused databases, but the data they provide nonetheless reveals information about an individual's location generally—their address, where they spend their time, who they spend time with, and other information. The data sold by these brokers includes publicly available information, consumer data, utility records, property records, social media information, and legal records.[69] Some of these data brokers also sell databases used for credit score reporting.[70]

Some of the companies selling access to this information—most notably Thomson Reuter's CLEAR, and LexisNexis's Accurint—also provide access to a data analytics software. These software programs can search through extensive databases and datasets, draw connections between data, and connect the data. DHS agents can use these tools to aggregate data across numerous sources and generate digital profiles of their targets with ease.[71]

**WHICH AGENCIES USE THEM:** Both ICE and CBP.

**DIRECT SURVEILLANCE OR DATA PURCHASES:** Data purchases.

**WHAT COMPANIES ARE SELLING THEM:** Giant Oak; Griffeye; ShadowDragon; Thomson Reuters (CLEAR) (until February 2021);[72] Equifax (collecting information from the National Consumer Telecom & Utilities Exchange (NCTUE), which itself obtains data from numerous technology and utility companies);[73] Lexis Nexis Accurint;[74] Babel Street (Babel X);[75] SmartyStreets;[76] Maltego;[77] Tableau.[78]

**HOW ICE AND/OR CBP ARE USING THEM:** ICE and CBP contract with numerous data brokers and publicly disclose limited information about what data they obtain from these brokers and how that data is used. Vendors like Thomson Reuters (CLEAR), ShadowDragon (SocialNet), Babel Street (Babel X), Giant Oak, Griffeye, and LexisNexis (Accurint) aggregate data from multiple sources and provide software that helps ICE and CBP analyze data. ShadowDragon's SocialNet relies primarily on social media sites and other websites to profile individuals, their relationships, and their locations. Babel Street's Babel X analyzes social media data and non-English data, providing analytical features including geospatial analysis, keyword filtering, and pattern identification. Thomson

Reuter's CLEAR and LexisNexis's Accurint aggregate billions of utility records, property records, license plate information, and other datapoints and provide advanced data search features.

**HOW DATA IS STORED:** Data from commercial data brokers is sometimes integrated into internal DHS databases. Other times, the data may be accessed by ICE or CBP agents utilizing an external software from the data broker or by agents sending the vendor lists of individuals to investigate.

# STORAGE & DISSEMINATION OF LOCATION INFORMATION ACROSS DHS RECORDS SYSTEMS

After location information is collected from individuals, it can travel through a complex web of databases accessed and shared by federal agencies, state and local agencies, and commercial data brokers. Exactly what information is in which databases has not been fully disclosed to the public; however, DHS privacy publications and FOIA disclosures point to several key databases that are confirmed to or likely to store location information.

There are three principal types of databases used by ICE and CBP that contain location information: (1) external databases that ICE and/or CBP users can access but are not owned by DHS, (2) internal ICE and/or CBP search and analysis tools that ingest data from other DHS databases, and (3) internal databases without advanced analysis capabilities that may also ingest data from other sources.

Databases that store mobile application location data comprise the first category. ICE and CBP do not store information from data brokers that sell mobile location data (i.e., Venntel and Babel Street) in DHS systems. Those data brokers provide ICE and CBP agents with access to an exclusively web-based application through which they can search and view location data from cell phones, Fitbits, and ankle monitors.

The second category—internal DHS databases with advanced analytical capabilities—includes the FALCON Search & Analysis System (FALCON-SA), the CBP Analytical Framework for Intelligence (AFI), ICE Investigative Case Management (ICM), the ICE Data Analysis System (DAS), the Intelligence Fusion System (IFS), and ICE Pattern Analysis and Information Collection (ICEPIC).

The third category—traditional databases without advanced analysis capabilities—includes TECS, the Electronic Surveillance System (ELSUR), ICE External Investigations System of Records, and the ICE Intelligence Records System (IIRS).

## FALCON SEARCH & ANALYSIS SYSTEM (FALCON-SA)

**WHAT IT IS:** ICE HSI uses the FALCON Search & Analysis System (FALCON-SA) as a data analysis and data organization tool for criminal and civil investigations. The tool can search through databases, identify relationships among data in different records systems, and "forecast patterns" based on that data.[79] FALCON software was developed for ICE by Palantir Technologies.[80] It is a version of Palantir's "Gotham" product.[81]

**LOCATION INFORMATION INCLUDED IN DATABASE:** FALCON-SA has wide-reaching access to data from government and commercial databases, and ICE agents can also import files manually into the system. FALCON-SA receives "GPS ping data" that it can analyze using "[m]apping" tools, "[t]imeline[s]," and "[g]eospatial [s]earches."[82] Other data collected by the system includes numerous forms of personal information, including "residential and work addresses . . . family relationships, employment . . . education and other background information."[83] FALCON-SA also contains information from commercial data brokers, including CLEAR.[84]

**NOTABLE SUB-RECORDS:** FALCON-SA receives information from other DHS records systems. These include the ICE Intelligence Records System (IIRS); the ICE External Investigations system; TECS; ICE's Immigration and Enforcement Operations Records System (ENFORCE); [85] ICE's Enforcement Integrated Database; [86] CBP's Analytical Framework for Intelligence; and CBP's Automated Targeting System.[87]

**DATA USE, STORAGE, AND SHARING:** While the FALCON-SA system absorbs data from multiple systems, the FALCON-SA system itself is only accessible to certain ICE personnel. Specifically, "ICE users" generally only includes ICE HSI agents; however, it can also include contractors, members of task forces, and other agency officials assigned to ICE HSI.[88]

Although the FALCON-SA system is only available to ICE HSI personnel, ICE may produce reports based on information generated through FALCON-SA, and those reports can be shared externally—including with local law enforcement and foreign agencies.[89]

Data that Falcon-SA accesses from other DHS databases is stored "for the same length of time as the source DHS system."[90] Manually-uploaded data not associated with a case is stored for 20 years, unless an exception applies. Data visualizations and searches are stored for 30 years unless they are associated with a particular case.[91]

## ANALYTICAL FRAMEWORK FOR INTELLIGENCE (AFI)

**WHAT IT IS:** The Analytical Framework for Intelligence (AFI) is a data analysis tool used by CBP. AFI users can search numerous DHS and federal databases, as well as data from commercial vendors. AFI has several analytic capabilities, including the ability to draw connections and patterns among information and to perform geospatial analysis, which "can help produce intelligence about the location or type of location that is favorable for a particular activity."[92]

**LOCATION INFORMATION INCLUDED IN DATABASE:** AFI compiles numerous forms of data from diverse sources including biographic data on individuals, vehicle data, and DMV data.[93] AFI also obtains "identity and imagery data" from commercial data brokers, including geospatial data that it uses to "support visualization of the data on maps."[94]

**NOTABLE SUB-RECORDS:** AFI absorbs information from numerous federal databases. Notable sub-records include TECS (a CBP system discussed below), the FBI Terrorist Screening Database, the Immigration and Enforcement Operational Records (ENFORCE), and the Automated Targeting System.[95] AFI also receives intelligence data from the **CBP Intelligence Records System (CIRS)** and processes the information, and CIRS stores the processed intelligence information.[96]

CBP's **Automated Targeting System (ATS)** is a data analysis and "decision support tool" used by CBP to process information about travelers and cargo.[97] ATS collects large amounts of information related to border crossings, and this information includes license plate information from state DMVs.[98] ATS also analyzes suspects' personal information (including addresses), and it receives real-time data from other federal databases including the FBI's Terrorist Screening Database.[99]

**DATA USE, STORAGE, AND SHARING:** Those with a TECS profile (a CBP system discussed below) can access TECS data, including data that comes from commercial data vendors.[100] Data not stored in TECS requires additional authorization to view.[101] "Finished intelligence products" or intelligence work that is completed by DHS employees, that use AFI can be shared internally within DHS and externally with other law enforcement agencies.[102]

AFI "projects" are retained for "up to 30 years," requests for information and their responses for 10 years, and "finished intelligence products" for 20 years.[103]

## ICE DATA ANALYSIS SYSTEM (DAS)

**WHAT IT IS:** The ICE Data Analysis System (DAS) is "an analytical database owned, operated, and maintained" by ICE Enforcement and Removal Operations (ERO).[104] Within ICE ERO, DAS is primarily used by the National Criminal Analysis and Targeting Center (NCATC), which uses surveillance to develop new leads for ICE immigration enforcement targets.[105]

**LOCATION INFORMATION INCLUDED IN DATABASE:** DAS contains biographic data about individuals, including their addresses and driver's license numbers, their vehicle information and license plate numbers, and other information.[106] DAS also obtains address information from the USPS.[107] Commercial vendors provide DAS with information that includes biographical information and vehicle information and may include other information.[108] DAS primarily includes information about noncitizens, but also includes some information about U.S. citizens.[109]

**NOTABLE SUB-RECORDS:** ICE compiles data from multiple sources internal and external to DHS, including, for example: **ICE's Enforcement Integrated Database** (discussed below), a database from the California Department of Corrections, the FBI Interstate Identification Index, and "publicly available data from two commercial sources."[110]

**DATA USE, STORAGE, AND SHARING:** ICE uses DAS to determine which noncitizens are eligible for deportation. An ICE agent from an ERO office sends NCATC a list of noncitizens in certain states that were recently granted parole, and a NCATC agent will then use DAS to determine which noncitizens ICE can deport.[111] "On a weekly basis," NCATC will also send commercial data brokers a list of noncitizens, and the commercial vendor responds with information on the individuals, which NCATC then uploads into DAS.[112] ICE reports that it "does not rely solely on address information obtained from commercial data sources" without verifying the data by other means.[113]

DAS stores the records it collects from other federal systems for a maximum of "3 months." [114] In 2017, ICE was in the process of developing a data storage schedule for other data in DAS.

Only a subset of ERO employees within the NCATC can use and interact with DAS. Other members of the NCATC may have read-only access to the database.[115] When NCATC reaches out to commercial data brokers seeking information about certain noncitizens, it provides those data brokers the names and dates of birth of the noncitizens.[116] ICE

shares DAS information with other DHS agencies, as well as other federal and international agencies in limited circumstances.[117]

## ICE PATTERN ANALYSIS AND INFORMATION COLLECTION (ICEPIC)

**WHAT IT IS:** ICEPIC is a data analysis tool that "allows ICE law enforcement agents and analysts to look for non-obvious relationship patterns among individuals and organizations."[118] ICE uses the tool to develop new leads and build upon existing ICE.[119]

**LOCATION INFORMATION INCLUDED IN DATABASE:** ICEPIC includes numerous types of personal identification information, including addresses, driver's license numbers, and affiliations. ICEPIC also obtains personal and biographic information from commercial data brokers.[120]

**NOTABLE SUB-RECORDS:** ICEPIC receives immigration violation information from DHS Enforcement Integrated Database.[121]

**DATA USE, STORAGE, AND SHARING:** ICEPIC is used in law enforcement and terrorism investigations. ICEPIC discloses information to other DHS agencies. Information from ICEPIC can be disclosed outside of DHS in certain circumstances, including to other federal, state, local, and foreign agencies for law enforcement purposes, and to intelligence agencies and foreign governments in terrorism cases.[122]

## ICE INVESTIGATIVE CASE MANAGEMENT (ICM)

**WHAT IT IS:** Investigative Case Management (ICM) is a new case management tool used by ICE to manage criminal and civil cases. The tool replaced ICE's use of the former TECS records system (but a new version of CBP TECS persists).[123] Palantir Technologies developed ICM FOR ICE.[124]

**LOCATION INFORMATION INCLUDED IN DATABASE:** ICM includes diverse information about individuals under investigation by ICE, including personal and biographic information. Also included among this information is location information, including information about use of location-tracking technologies, location data, license plate reader data, and telecommunications information.[125] Spreadsheets with information derived from location surveillance—including location data and device tracking numbers—are stored within ICM.[126] LPR data is stored in ICM "only in the context of individual case files."[127]

**NOTABLE SUB-RECORDS:** ICE agents will submit **ELSUR (Electronic Surveillance System)** requests to their supervisors before conducting electronic surveillance, and those ELSURs and related documents are stored in ICM.[128]

ICM users can also search numerous DHS databases from within the ICM, including: ICE Enforcement Integrated Database, CBP TECS, and CBP ATS.

**DATA USE, STORAGE, AND SHARING:** ICE HSI is the primary user of ICM, but according to an earlier Privacy Impact Assessment for ICM, ICE ERO previously "use[d] ICM to manage immigration cases that [were] presented for criminal prosecution."[129]

ICM includes information on "targets of investigations, associates of targets, victims, witnesses, informants and other third parties."[130] ICM contains numerous types of data, including evidentiary information and location data.[131] ICM does not store data from data brokers directly, but commercial data can be incorporated into reports, photos, and spreadsheets which, in turn, may be uploaded into ICM.[132]

ICM records are stored for 20 years.[133] ICM "Subject Records," or case files on individuals are shared with "external federal, state, local, tribal and international law enforcement agency partners' through the **Law Enforcement Information Sharing Service (LEIS)**."[134]

## CBP TECS

**WHAT IT IS:** TECS is a records system used by CBP officers at borders to screen arriving travelers. The acronym "TECS" formerly stood for "Treasury Enforcement Communications System."[135] A version of TECS used by both ICE and CBP was replaced in 2016 by ICM for ICE, and "CBP TECS Platform" for CBP. The new CBP TECS contains "the same type of information" as the former TECS.[136]

**LOCATION INFORMATION INCLUDED IN DATABASE:** TECS includes identification and travel information about individuals crossing the border (including via U.S. airports). Included among this information is license plate numbers of all vehicles that enter or leave the United States.[137] In addition to CBP inputting information into TECS, information in TECS can also come from other law enforcement agencies or the FBI's Terrorist Screening Database.[138]

**NOTABLE SUB-RECORDS:** Some authorized CBP TECS users can access **Nlets**. Nlets is a system owned by state agencies and used for information-sharing among states, local governments, and the federal government. The system includes drivers license, vehicle, and criminal history information. ICE, including ICE ERO, receives bulk DMV data primarily through Nlets, and this DMV information can reveal a person's address, photos, vehicle registration, and driver's license number.[139]

Data in TECS also comes from the **FBI's Terrorist Screening Database**, also known as the "terrorist watch list." The database receives data from and shares data with the CBP, the State Department, TSA, and state and local law enforcement. The database consolidates information used to identify individuals who "hav[e] an association with terrorism."[140] The Terrorist Screening Database has been frequently criticized for enabling the profiling of Muslims and other minorities.[141]

TECS also receives data from the **DHS Enforcement Integrated Database (EID)**, a records system that contains all data from the **"ENFORCE applications**."[142] The database stores all information relevant to ICE and CBP's immigration enforcement investigations, detentions, and deportations. The database contains numerous forms of personal and biographic information of individuals being investigated by DHS, including names, addresses, affiliations, and other information.[143]

**DATA USE, STORAGE, AND SHARING:** TECS is shared with other DHS agencies: ICE, USCIS, the Coast Guard, the Secret Service, the Visitor and Immigrant Status Indicator Technology, the DHS inspector General, TSA, and the Office of Intelligence and Analysis.

TECS data is integrated into a number of other databases, including FALCON-SA and AFI. Records in TECS can be stored for 75 years.[144]

## ELECTRONIC SURVEILLANCE SYSTEM (ELSUR)

**WHAT IT IS:** ELSUR is a records system that stores information concerning requests ICE has made to courts to obtain a warrant to surveil a person or other target.

**LOCATION INFORMATION INCLUDED IN DATABASE:** ELSUR stores information regarding both successful and unsuccessful surveillance requests, as well as "information about subjects, target devices, locations, [and] vehicles."[145] Information about target devices can include a cell phone's device identification number, and location records can include a person's home address.[146]

Information in ELSUR comes from other ICE and other federal agency records. According to ICE, the system does not use commercial or publicly available data.[147]

**DATA USE, STORAGE, AND SHARING:** When federal agencies seek a warrant from a court in order to surveil a target for a criminal investigation, they are required by law to "search their own records of previous . . . requests and those of other agencies that may have investigated those same subjects in the past," and inform the court if there have been prior attempts to surveil that target.[148] As such, ICE shares ELSUR information with other federal agencies to assist those agencies with preparing their own surveillance requests.[149] ICE stores information in ELSUR for 50 years.[150]

## ICE INTELLIGENCE RECORDS SYSTEM (IIRS)

**WHAT IT IS:** IIRS is a records system used by ICE for immigration enforcement and criminal enforcement investigations. IIRS enables information dissemination between ICE and state and local law enforcement agencies.[151]

**INFORMATION INCLUDED IN DATABASE:** Individuals whose information is included in the database include people who are suspected of terrorism or gang membership.[152] It also includes "subjects, witnesses, [and] associates" who are connected to ICE investigations or ICE enforcement—even if those individuals are only connected to investigations conducted by other law enforcement agencies (state, local, or foreign) "where there is a potential nexus" to ICE's work "or homeland security in general."[153] Information about subjects of intelligence reports is also included in the database.

**LOCATION INFORMATION INCLUDED IN THE DATABASE:** IIRS might include some data revealing location. IIRS contains fifteen categories of information about individuals. These categories include biographic information; immigration enforcement and immigration investigative records; visa, immigration, and arrival and departure data; records related to individuals suspected of terrorism; intelligence reports; gang affiliation; and other information.[154]

**NOTABLE SUB-RECORDS:** Within IIRS is "**ICEGangs**," a database of suspected gang members. The database includes personally identifying information of suspects, including their immigration status, photos, government ID numbers, and biographic information.[155] ICE gives California Department of Justice users access to ICEGangs and "anticipates" sharing the database with other state and local agencies.[156]

Another sub-record within IIRS is "**Intelligence Fusion System**" (IFS) (formerly the ICE Network Law Enforcement Analysis Data System). IFS is a search tool operated by ICE and used for immigration enforcement, intelligence, and investigations.[157]

**DATA USE, STORAGE, AND SHARING:** Falcon Search & Analysis (FALCON-SA) receives data from IIRS. Intelligence Fusion System (IFS)'s is housed within IIRS.[158] Records from IIRS can also be disclosed to other agencies including local, state, and foreign to assist them in their law enforcement work; with foreign governments for intelligence or counterterrorism purposes; and for other uses. ICEGangs is shared with the California Department of Justice and likely other state and local law enforcement agencies.

## INTELLIGENCE FUSION SYSTEM (IFS)

**WHAT IT IS:** The "Intelligence Fusion System" (IFS) is a search tool used by ICE and CBP for immigration enforcement, intelligence, and investigations. Like FALCON-SA, IFS analyzes data from multiple data sources. Its analytical capabilities include being able to search multiple sets of data efficiently and identify links between data and relationships between people. IFS also uses maps and Google satellite data to visually map the locations of individuals.[159] For the ICE Office of Intelligence, IFS is also a tool used for creating and storing intelligence reports.[160]

**LOCATION INFORMATION INCLUDED IN DATABASE:** IFS collects records from DHS, other federal agencies, state agencies, local agencies, and open-source data from data brokers and websites.[161] Information in IFS includes personal identifying information on individuals; visa, border, and immigration data; "DHS immigration and law enforcement" information; information about the terrorist watchlist; and other data.[162]

**DATA USE, STORAGE, AND SHARING:** IFS contains personal identifying information on all individuals covered by IIRS in addition to several categories of people. These categories include individuals identified in law enforcement reports and incident reports and individuals identified in DHS records concerning immigration and law enforcement.[163]

IFS does not provide other agencies with search privileges, but it may share information with federal, state, local, foreign, and international agencies "that demonstrate[] a need to know."[164]

## ICE EXTERNAL INVESTIGATIONS SYSTEM OF RECORDS

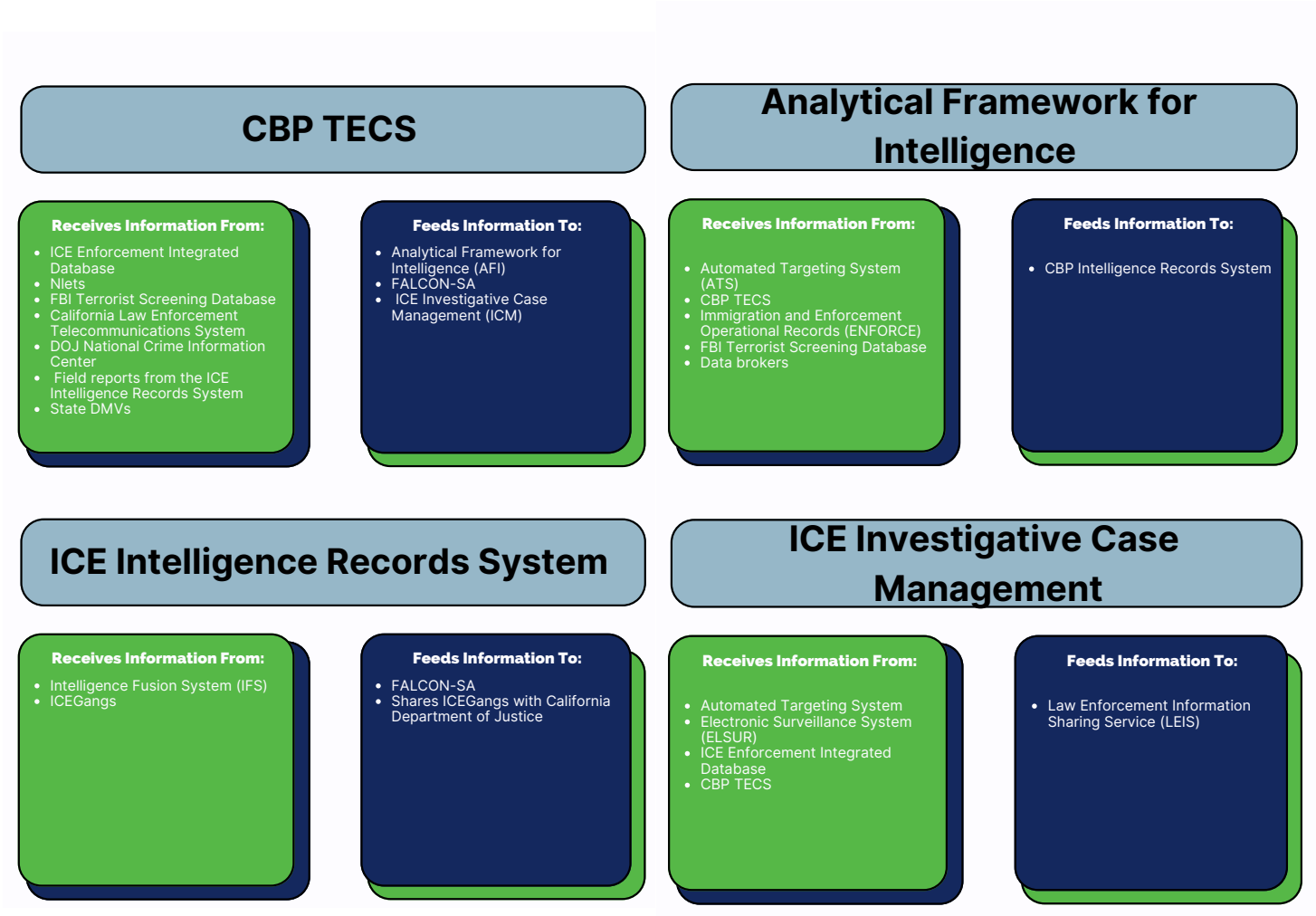
**WHAT IT IS:** ICE's External Investigation System of Records is a system that primarily houses records related to external investigations conducted by ICE HSI.[165]

**LOCATION INFORMATION INCLUDED IN DATABASE:** The records in this database include personal information about subjects, associates, victims, and witnesses; location tracking information; and evidentiary records including travel history, surveillance reports, and telecommunications data.[166] ICE not only collects information about individuals who they investigate for violating U.S. immigration or criminal laws, but the agency also collects information on "family members and known associates" of those subjects.[167] The location records ICE houses in this system include information from location tracking devices that use GPS and cell-site towers, as well as location information from license plate readers.[168]

**DATA USE, STORAGE, AND SHARING:** ICE shares these records with DHS agencies, as well as with other federal, state, local, and foreign agencies in limited circumstances.[169] Records are retained for 20 years.[170]

# SUMMARY: INFORMATION FLOW AMONG RECORDS SYSTEMS

Below is a summary of major ICE and CBP records systems containing location information. The diagrams highlight some of the systems from which they receive location information, as well as some of the systems to which they feed information.



## FALCON-SA

**Receives Information From:**

- Analytical Framework for Intelligence (AFI)
- Automated Targeting System (ATS)
- CBP TECS
- ENFORCE
- ICE Enforcement Integrated Database
- Intelligence Records System (IIRS)
- ICE External Investigations System
- Data brokers

## Intelligence Fusion System

**Receives Information From:**

- CBP TECS
- ENFORCE
- Intelligence reports from the ICE Office of Intelligence
- Data brokers

**Feeds Information To:**

- ICE Intelligence Records System (IIRS)

## ICE Data Analysis System

**Receives Information From:**

- ICE Enforcement Integrated Database
- FBI Interstate Identification Index
- USPS
- California Department of Corrections
- Data brokers

## ICE External Investigations System of Records

**Feeds Information To:**

- Shares data with other DHS components and agencies in limited circumstances

## ICE Pattern Analysis & Information Collection (ICEPIC)

**Receives Information From:**

- CBP TECS
- ICE Enforcement Integrated Database
- ICE External Investigations System
- ICE Intelligence Records System (IIRS)
- Data brokers

## Electronic Surveillance System (ELSUR)

**Feeds Information To:**

- ICE Investigative Case Management (ICM)

# POLICY RECOMMENDATIONS

All surveillance and dissemination of individuals' personal information threatens privacy rights and civil liberties. When that surveillance and information dissemination targets already-marginalized populations like immigrants and migrants, the consequences are all the graver—making these populations vulnerable to a disproportionate amount of policing, confinement, and control. The following are initial policy steps that DHS and other agencies should adopt to lessen the privacy rights violations endemic to current policy. Adopting these recommendations would be a mere preliminary step toward fulfilling international privacy standards and toward ending all domestic surveillance of immigrants.

1) **END PURCHASES FROM OR SUBSCRIPTIONS TO COMMERCIAL DATA BROKERS AND REQUIRE A WARRANT BEFORE ACCESSING SENSITIVE LOCATION DATA.** The Supreme Court's 2018 decision in *United States v. Carpenter* made it unlawful for the government to obtain historical cell-site location information without a warrant.[171] Since that decision, DHS has used data brokers selling mobile location data as a loophole to the Supreme Court's prohibition, purchasing mobile location information from commercial vendors without obtaining a judicial warrant for probable cause. This constitutionality of this workaround is questionable, and at the very least the practice is contrary to the spirit of the Fourth Amendment.

   DHS use of commercial data brokers has also, at times, contravened the spirit of local sanctuary provisions.[172] DHS should respect the decisions of state and local governments that have chosen, through their democratic process, to institute sanctuary provisions and limit information-sharing with DHS. DHS should end its practice of bypassing local sanctuary laws.

   DHS should voluntarily end its contracts with commercial data brokers and instate a policy requiring a judicial warrant before obtaining or accessing all precise geolocation information, including information from GPS trackers, cell-site simulators, and smartphones. As DHS has thus far failed to voluntarily instate these policies, Congress should pass the **Fourth Amendment Is Not for Sale Act**.[173] The Fourth Amendment Is Not for Sale Act would require the government to obtain a warrant before obtaining personal data from data brokers.[174] The Act has been endorsed by our partner privacy rights advocates.[175]

2) **MINIMIZE BULK COLLECTION AND TRANSFERS OF LOCATION DATA, AND END USE OF SENSITIVE LOCATION DATA FOR DEVELOPMENT OF NEW LEADS**. ICE and CBP should end the practice of collecting and disseminating personal information in a massive scale or in a routine manner and using that information for immigration enforcement and investigations. ICE and CBP collect sensitive information on a massive scale from commercial data brokers and from other agencies such as state DMVs, local law enforcement agencies, and the FBI. Location information and other personal information is amassed by the ICE Data Analysis System and used to generate new leads for deportations—civil violations. ICE and CBP have purchased data tools like CLEAR, ShadowDragon, and FALCON-SA that are specifically designed to digest scores of personal data. The agencies have also developed information channels with other federal agencies and with state and local agencies through systems like the Intelligence Fusion System to make it easier to circulate individuals' personal data among many entities.

   ICE and CBP must end the collection and storage of sensitive personal information in a routine or mass scale for immigration enforcement and investigations. ICE and CBP should not use TECS, which contains routine traveler data, and similar routine databases for their investigations and enforcement. The agencies must also end the practice of purchasing access to databases that amass large amounts of personal data. Further, ICE and CBP should end requests of bulk information transfers from non-federal entities like state DMVs. If DHS must obtain personal information about an individual, that information should only be sought in exceptional, high-priority investigations involving serious criminal liability. Moreover, ICE or CBP should end use of location information for deportations and for civil cases involving mere violations of immigration regulations. ICE and CBP must end the use of location information to develop new leads for their investigations—neither for their criminal nor civil cases.

3) **LIMIT STORAGE OF SENSITIVE DATA.** DHS should limit the length of time it retains sensitive data, particularly its storage of data in the Falcon-SA system, ELSUR, ICM, and TECS—all of which store data for decades. At a minimum, however, DHS should add provisions to contracts with commercial data vendors implementing routine audits of retention limits and deletion policies. Any storage limits DHS imposes on location data it stores internally should be imposed on contractors who provide DHS with subscriptions to data. DHS should also add contractual provisions that limit or prohibit any combination of personal data from DHS with vendor data.

4) **DHS MUST DISCLOSE COMMERCIAL DATABASES THAT IT ACCESSES BUT DOES NOT STORE INTERNALLY.** Under DHS's contracts with data brokers Venntel and Babel Street for mobile location data, DHS obtains access to an entirely web-based database of geolocation

information, without any records stored in DHS system. Because no records are stored within DHS, DHS has neither published a Systems of Records Notice nor a Privacy Impact Assessment concerning the geolocation databases it accesses.

The Privacy Act requires a System of Records Notice when a federal agency maintains records that "contain information about an individual" and that are "retrieved by a personal identifier."[176] The E-Government Act requires Privacy Impact Assessments when agencies incorporate commercial databases into their systems, but does not require one when agencies "[m]erely query[] such a source on an ad hoc basis using existing technology."[177] By keeping mobile location databases external to DHS systems, DHS has evaded the disclosures it would ordinarily be required to perform by the Privacy Act and E-Government Act. DHS must end these loopholes by disclosing not only the databases of personal data that it stores internally within its systems, but also disclosing any databases of personal information to which it has access.

5) **DHS MUST CONSIDER PRECISE LOCATION INFORMATION TO BE "PERSONALLY IDENTIFIABLE INFORMATION" AND COMPLY WITH THE PRIVACY IMPACT ASSSESMENT REQUIREMENT OF THE E-GOVERNMENT ACT.** DHS claims that the precise location information it obtains from data brokers like Venntel and Babel Street is not personally identifiable information (PII) because it is anonymized.[178] However, studies have shown that anonymized geolocation data is not truly anonymous.[179] Moreover, location information about individuals is considered to be personal information "under most, if not all, privacy laws around the world."[180]

DHS is required under the E-Government Act to conduct a Privacy Impact Analysis for acquisitions of PII from more than 10 people.[181] DHS may be strategically categorizing anonymized location data as non-PII to evade its obligation to publish a Privacy Impact Analysis for its acquisition of the data. DHS must change its policy to recognize precise location information as PII even when it is anonymized. Location data information is incredibly sensitive and revealing, and, when acquired by ICE and CBP, the agencies must take the necessary steps to protect privacy rights.

### 6) END SURVEILLANCE AS AN "ALTERNATIVE" TO OTHER METHODS OF CONTROL.

Surveillance and sensitive data collection are not "humane" alternatives to other methods of controlling the border or monitoring immigrants. Surveillance is a method of control that harms fundamental rights to privacy and autonomy. DHS, therefore, should end its adoption of the so-called "smart wall" as a surveillance-based alternative to border control.[182] ICE should also end its surveillance under the "Alternatives to Detention" program. Surveillance under that program is not a "humane alternative" to detention, and the system surveils more immigrants and asylum seekers than would otherwise have faced detention.[183] In the alternative, ICE should look to the recommendations of immigrant justice advocates who provide guidance on best practices for immigration case management that do not involve surveillance.[184]

[1] *See, e.g.*, AMERICAN DRAGNET: DATA-DRIVEN DEPORTATION IN THE 21ST CENTURY, CTR. ON PRIVACY & TECH. (2022), https://americandragnet.org; THE DATA BROKER TO DEPORTATION PIPELINE: HOW THOMSON REUTERS & LEXISNEXIS SHARE UTILITY & COMMERCIAL DATA WITH ICE, JUST FUTURES L. & MIJENTE, https://www.flipsnack.com/justfutures/commercial-and-utility-data-report/full-view.html; UNTANGLING THE IMMIGRATION ENFORCEMENT WEB: BASIC INFORMATION FOR ADVOCATES ABOUT DATABASES AND INFORMATION-SHARING AMONG FEDERAL, STATE, AND LOCAL AGENCIES, NAT'L IMMIGR. L. CTR. (2017), https://www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf.

[2] CELL SITE SIMULATORS, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS (2015), https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-4-28_Cell-Site-Simulator-Primer_Final.pdf.

[3] Minh Tran, WHITE PAPER - ACCURATE LOCATION DETECTION: 911 SMS HELP APP (May 2015), https://transition.fcc.gov/pshs/911/Apps%20Wrkshp%202015/911_Help_SMS_WhitePaper0515.pdf/

[4] *See generally* GOTTA CATCH 'EM ALL, ELECTRONIC FRONTIER FOUND. (2019), https://www.eff.org/files/2019/07/09/whitepaper_imsicatchers_eff_0.pdf; *Stingray Tracking Devices: Who's Got Them?*, ACLU (Nov. 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them#:~:text=Stingrays%2C%20also%20known%20as%20%22cell,their%20locations%20and%20identifying%20information.

[5] *Purchase Order*, PIID HSCEMD11P00196, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSCEMD11P00196_7012_-NONE-_-NONE-; *Purchase Order*, PIID HSCEMD11P00245, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSCEMD11P00245_7012_-NONE-_-NONE-; *Purchase Order*, PIID HSCEMD11P00267, https://www.usaspending.gov/award/CONT_AWD_HSCEMD11P00267_7012_-NONE-_-NONE-.

[6] *See ICE and CBP Are Secretly Tracking Us Using Stingrays. We're Suing*, ACLU (Dec. 11, 2019), https://www.aclusocal.org/en/news/ice-and-cbp-are-secretly-tracking-us-using-stingrays-were-suing.

[7] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[8] PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND SECURITY INVESTIGATION (HIS) SURVEILLANCE TECHNOLOGIES 7, DHS/ICE/PIA-061 (Jan. 24, 2022), https://www.dhs.gov/sites/default/files/2022-01/privacy-pia-ice061-hsisuveillancetech-january2022_0.pdf.

[9] *Id*.

[10] Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

[11] *See id*.

[12] *Privacy Policy*, VENNTEL (Nov. 2021), https://www.venntel.com/privacy-policy.

[13] For more information on geolocation data generation and Ad-IDs, see LEGAL LOOPHOLES AND DATA FOR DOLLARS: HOW LAW ENFORCEMENT AND INTELLIGENCE AGENCIES ARE BUYING YOUR DATA FROM BROKERS 22-23, CTR. FOR DEMOCRACY & TECH. (2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

[14] *CBP's First Production: ACLU v. Department of Homeland Security (commercial location data FOIA)*, ACLU, at 16, https://www.aclu.org/legal-document/cbps-first-production; *CBP's Fourth Production: ACLU v. Department of Homeland Security (commercial location data FOIA)*, ACLU, at 100-01, https://www.aclu.org/legal-document/cbps-fourth-production.

[15] *See* Joseph Cox, *Customs and Border Protection Paid $476,000 to a Location Data Firm in New Deal*, VICE MOTHERBOARD (Aug. 25, 2020), https://www.vice.com/en/article/k7qyv3/customs-border-protection-venntel-location-data-dhs.

[16] *ICE's May 2021 Production: ACLU v. Department of Homeland Security (commercial location data FOIA)*, ACLU, at 205, https://www.aclu.org/legal-document/ices-may-2021-production (Privacy Threshold Analysis stating that

"because query results do not produce the name or other contact information of an individual, ICE users must serve the geolocation data service provider with a subpoena to obtain the identity of the individual that owns the digital device").

[17] For example, in ICE's Procurement Checklist for acquiring a Venntel subscription, ICE checked the box stating that the vendor will not have the ability to view PII. The list of PII examples on the checklist does not include location information. *See ICE's May 2021 Production: ACLU v. Department of Homeland Security (commercial location data FOIA)*, ACLU, at 199, https://www.aclu.org/legal-document/ices-may-2021-production.

[18] *See* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html ("Describing location data as anonymous is 'a completely false claim' that has been debunked in multiple studies . . . ."); Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data*, TECHCRUNCH (July 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data (summarizing studies); Chris Riederer et al., *Linking Users Across Domains with Location Data: Theory and Validation*, IW3C2 (Apr. 11-15, 2016), http://www.cs.columbia.edu/~mani/pub/RiedererWWW2016.pdf.

[19] Samuel N. Eshun & Paolo Palmieri, *Two De-Anonymization Attacks on Real-World Location Data Based on a Hidden Markov Model*, IEEE (2022), https://ieeexplore.ieee.org/abstract/document/9799345/authors#authors.

[20] *See, e.g.*, *CBP's Third Production: ACLU v. Department of Homeland Security (commercial location data FOIA)*, ACLU, at 25-28, https://www.aclu.org/legal-document/cbps-third-production.

[21] *Id.*; *see also Cox*, *Customs and Border Protection Paid $476,000 to a Location Data Firm in New Deal*, *supra* note 15.

[22] *ICE's May 2021 Production: ACLU v. Department of Homeland Security (commercial location data FOIA)*, *supra* note 16, at 158.

[23] HSI procured Gravy Analytics so for data analysis in human smuggling and trafficking investigations "globally and within the United States." *ICE's May 2021 Production: ACLU v. Department of Homeland Security (commercial location data FOIA)*, *supra* note 16, at 202.

[24] *Purchase Order*, PIID 70CMSD21P00000132, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CMSD21P00000132_7012_-NONE-_-NONE-.

[25] *Delivery Order*, PIID HSBP1016J00553, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSBP1016J00553_7014_HSSS0112D0002_7009.

[26] *Delivery Order*, PIID HSCEMD11J00108, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSCEMD11J00108_7012_HSCEMD10D00004_7012.

[27] *Purchase Order*, PIID 70B03C21P00000331, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70B03C21P00000331_7014_-NONE-_-NONE-.

[28] *Purchase Order*, PIID HSCENV08P00321, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSCENV08P00321_7012_-NONE-_-NONE-.

[29] *Delivery Order*, PIID HSCEMD12F00026, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSCEMD12F00026_7012_DJD11C0002_1524.

[30] *Delivery Order*, PIID HSCENV09F00045, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSCENV09F00045_7012_DJDEA05C0023_1524.

[31] *Delivery Order*, PIID HSBP9861713745, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSBP9861713745_7014_GS07F362AA_4732; *Delivery Order*, PIID HSBP9861828217, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSBP9861828217_7014_GS07F362AA_4732.

[32] *Purchase Order*, PIID 70CMSD21P00000112, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CMSD21P00000112_7012_-NONE-_-NONE-.

[33] *Purchase Order*, PIID 70B06C22P00000321, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70B06C22P00000321_7014_-NONE-_-NONE-.

[34] *Purchase Order*, PIID HSBP1013P00257, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSBP1013P00257_7014_-NONE-_-NONE-.

[35] *See infra* note 134 and accompanying text (discussing the Law Enforcement Information Sharing Service); PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND SECURITY INVESTIGATION (HIS) SURVEILLANCE TECHNOLOGIES, *supra* note 8, at 6.
[36] PRIVACY IMPACT ASSESSMENT FOR ICE INVESTIGATIVE CASE MANAGEMENT 13, DHS/ICE/PIA-045 (June 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf.
[37] *See* TRACKED & TRAPPED: EXPERIENCES FROM ICE DIGITAL PRISONS, MIJENTE ET AL. (2022), https://notechforice.com/wp-content/uploads/2022/05/TrackedTrapped_final.pdf; Giulia McDonnell, *Meet SmartLINK, the App Tracking Nearly a Quarter Million Immigrants*, DOCUMENTED (June 27, 2022), https://documentedny.com/2022/06/27/smartlink-app-tracking-immigrants-ice-privacy; *Epic & Coalition Endorse Congressional Letter to DHS Opposing Expansion of "E-Carceration,"* EPIC (Feb. 24, 2022), https://epic.org/epic-coalition-endorse-congressional-letter-to-dhs-opposing-expansion-of-e-carceration (linking a coalition letter to DHS Secretary Mayorkas regarding the ICE Intensive Supervision Appearance Program, https://epic.org/wp-content/uploads/2022/02/ICE-ISAP-Congressional-Letter_final.pdf).
[38] *See* TRACKED & TRAPPED: EXPERIENCES FROM ICE DIGITAL PRISONS, *supra* note 37; Giulia McDonnell, *Ankle Monitors and GPS Apps: ICE's Alternatives to Detention, Explained*, DOCUMENTED (Sept. 20, 2021), https://documentedny.com/2021/09/20/ankle-monitors-and-gps-apps-ices-alternatives-to-detention-explained.
[39] TRACKED & TRAPPED: EXPERIENCES FROM ICE DIGITAL PRISONS, MIJENTE ET AL., *supra* note 37, at 3; https://www.theguardian.com/us-news/2022/mar/14/us-immigration-surveillance-isap; *see* Johana Bhuiyan, *A US Surveillance Program Tracks Nearly 200,000 Immigrants. What Happens to Their Data?*, GUARDIAN (Mar. 14, 2022), https://www.theguardian.com/us-news/2022/mar/14/us-immigration-surveillance-isap.
[40] *See ICE's May 2021 Production: ACLU v. Department of Homeland Security (commercial location data FOIA)*, *supra* note 16, at 299-301.
[41] PRIVACY IMPACT ASSESSMENT FOR THE CBP ONE™ MOBILE APPLICATION 2, DHS/CBP/PIA-068, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp068-cbpmobileapplication-may2021.pdf.
[42] *Id*. at 9-10.
[43] *See ICE's May 2021 Production: ACLU v. Department of Homeland Security (commercial location data FOIA)*, *supra* note 16, at 384-85, 400; *CBP's Fifth Production: ACLU v. Department of Homeland Security (commercial location data FOIA)*, ACLU, at 77, https://www.aclu.org/legal-document/cbps-fifth-production.
[44] *See* PRIVACY IMPACT ASSESSMENT FOR ICE INVESTIGATIVE CASE MANAGEMENT, *supra* note 36, at 10-11.
[45] *Id*. at 29.
[46] *See* PRIVACY IMPACT ASSESSMENT FOR THE CBP ONE™ MOBILE APPLICATION, *supra* note 41, at 11.
[47] *See Street-Level Surveillance: Automated License Plate Readers (ALPRs)*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/automated-license-plate-readers-alpr.
[48] *Purchase Order*, PIID 70B03C21P00000306, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70B03C21P00000306_7014_-NONE-_-NONE-.
[49] *See* THE DATA BROKER TO DEPORTATION PIPELINE, *supra* note 1, at 8; *Purchase Order*, PIID HSBP1015P00498, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSBP1015P00498_7014_-NONE-_-NONE-; *Purchase Order*, PIID HSBP1016P00515, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSBP1016P00515_7014_-NONE-_-NONE-; *Purchase Order*, PIID HSCEMD11P00261, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSCEMD11P00261_7012_-NONE-_-NONE-.
[50] *Purchase Order*, PIID 70CDCR18P00000017, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CDCR18P00000017_7012_-NONE-_-NONE-.
[51] *Delivery Order*, PIID HSCEMD10F00175, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSCEMD10F00175_7012_GS07F0073L_4730; *Delivery Order*, PIID 70CMSD21FR0000095, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CMSD21FR0000095_7012_GS07F0004Y_4732; *Purchase Order*, PIID 70CMSD21P00000073, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CMSD21P00000073_7012_-NONE-_-NONE-; *Delivery Order*,

PIID 70CMSD21FR0000103, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CMSD21FR0000103_7012_GS07F0004Y_4732.
[52] *Delivery Order*, PIID HSBP1015F00509, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSBP1015F00509_7014_GS10F0226W_4730
[53] *Purchase Order*, PIID 70B03C21P00000447, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70B03C21P00000447_7014_-NONE-_-NONE-; *Purchase Order*, PIID 70B03C20P00000447, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70B03C20P00000447_7014_-NONE-_-NONE-.
[54] *See* THE DATA BROKER TO DEPORTATION PIPELINE, *supra* note 1, at 7.
[55] *See* PRIVACY IMPACT ASSESSMENT FOR CBP LICENSE PLATE READER TECHNOLOGY 6, DHS/CBP/PIA-049 (Dec. 11, 2017), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp049-cbplprtechnology-december2017.pdf.
[56] *See* PRIVACY IMPACT ASSESSMENT FOR THE CBP LICENSE PLATE READER TECHNOLOGY 2, DHS/CBP/PIA-049(a) (July 6, 2020), https://www.dhs.gov/publication/dhscbppia-049-cbp-license-plate-reader-technology.
[57] *Id*. at 5.
[58] PRIVACY IMPACT ASSESSMENT UPDATE FOR THE AUTOMATED TARGETING SYSTEM 78, DHS/CBP/PIA-006(e) (Jan. 13, 2017), https://www.dhs.gov/sites/default/files/2022-05/privacy-pia-cbp006%28e%29-ats-may2022.pdf.
[59] PRIVACY IMPACT ASSESSMENT FOR ICE INVESTIGATIVE CASE MANAGEMENT, *supra* note 36, at 14.
[60] Covert LPRs are not used for "real-time hot list hits." PRIVACY IMPACT ASSESSMENT FOR CBP LICENSE PLATE READER TECHNOLOGY, *supra* note 56, at 6.
[61] PRIVACY IMPACT ASSESSMENT FOR ICE INVESTIGATIVE CASE MANAGEMENT, *supra* note 36, at 14.
[62] *See* PRIVACY IMPACT ASSESSMENT FOR THE ACQUISITION AND USE OF LICENSE PLATE READER (LPR) DATA FROM A COMMERCIAL SERVICE 2, DHS/ICE/PIA-039(b) (May 21, 2021), https://www.dhs.gov/sites/default/files/publications/privacy-pia30b-ice-acquisitionanduseoflprdatafromacommercialservice-june2021_0.pdf.
[63] *Id*. at 1-3.
[64] *Id*. at 3.
[65] *See* PRIVACY IMPACT ASSESSMENT FOR THE ACQUISITION AND USE OF LICENSE PLATE READER (LPR) DATA FROM A COMMERCIAL SERVICE, *supra* note 62, at 15.
[66] *See* PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND SECURITY INVESTIGATION (HIS) SURVEILLANCE TECHNOLOGIES, *supra* note 8, at 12; PRIVACY IMPACT ASSESSMENT FOR ICE INVESTIGATIVE CASE MANAGEMENT, *supra* note 36, at 14.
[67] PRIVACY IMPACT ASSESSMENT FOR THE ACQUISITION AND USE OF LICENSE PLATE READER (LPR) DATA FROM A COMMERCIAL SERVICE, *supra* note 62, at 9-10.
[68] PRIVACY IMPACT ASSESSMENT UPDATE FOR THE AUTOMATED TARGETING SYSTEM, *supra* note 58, at 86.
[69] *See* THE DATA BROKER TO DEPORTATION PIPELINE, *supra* note 1.
[70] *Id*. at 8.
[71] *Id*. at 7, 9.
[72] *See* THE DATA BROKER TO DEPORTATION Pipeline, *supra* note 1, at 7.
[73] *See* The Data Broker to Deportation Pipeline, *supra* note 1, at 6; *Purchase Order*, PIID 70CMSD20P00000187, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CMSD20P00000187_7012_-NONE-_-NONE-.
[74] *See* THE DATA BROKER TO DEPORTATION PIPELINE, *supra* note 1, at 7.
[75] *Delivery Order*, PIID 70B03C20F00001148, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70B03C20F00001148_7014_HSHQDC12D00013_7001.
[76] *Purchase Order*, PIID HSCETE17P00043, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSCETE17P00043_7012_-NONE-_-NONE-.
[77] *ICE's July 2021 Production (1): ACLU v. Department of Homeland Security (commercial location data FOIA)*, ACLU, at 284-85, https://www.aclu.org/legal-document/ices-july-2021-production-1 (ICE HSI emails describing Maltego that do not make clear whether ICE procured the technology).
[78] *Purchase Order*, PIID 70B06C20P00000272, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70B06C20P00000272_7014_-NONE-_-NONE-; *Delivery Order*, PIID 70CTD022FR0000131, USASPENDING,

https://www.usaspending.gov/award/CONT_AWD_70CTD022FR0000131_7012_HSHQDC12D00013_7001; *Delivery Order*, PIID 70CTD021FR0000142, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CTD021FR0000142_7012_HSHQDC12D00013_7001; *Delivery Order*, PIID 70B01C18F00001134, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70B01C18F00001134_7014_HSHQDC13D00020_7001; *Delivery Order*, PIID 70CTD019FR0000150, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CTD019FR0000150_7012_HSHQDC13D00010_7001; *Delivery Order*, PIID HSCETE17J00332, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_HSCETE17J00332_7012_HSHQDC12D00015_7001; *Delivery Order*, PIID 70CMSD22FR0000039, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CMSD22FR0000039_7012_HSHQDC12D00015_7001; *Delivery Order*, PIID 70CMSD21FR0000062, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CMSD21FR0000062_7012_HSHQDC12D00015_7001; *Delivery Order*, PIID 70CMSD20FR0000056, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CMSD20FR0000056_7012_HSHQDC12D00022_7001; *Purchase Order*, PIID 70CMSW19P00000023, USASPENDING, https://www.usaspending.gov/award/CONT_AWD_70CMSW19P00000023_7012_-NONE-_-NONE-.

[79] *2nd Interim Production: Part 2*, EPIC v. ICE (Palantir Databases), at 806-13, https://epic.org/wp-content/uploads/foia/dhs/ice/palantir-databases/EPIC-17-08-14-ICE-FOIA-20180420-2ndInterim-Production-pt2.pdf.

[80] *See FOIA Cases: EPIC v. ICE (Palantir Databases)*, EPIC, https://epic.org/documents/epic-v-ice-palantir-databases.

[81] *4th Interim Production: Part 3*, EPIC v. ICE (Palantir Databases), at 1723, https://epic.org/wp-content/uploads/foia/dhs/ice/palantir-databases/EPIC-17-08-14-ICE-FOIA-20180703-4thInterim-Production-pt3.pdf; *6th Interim Production: Part 2*, EPIC v. ICE (Palantir Databases), at 2696, https://epic.org/wp-content/uploads/foia/dhs/ice/palantir-databases/EPIC-17-08-14-ICE-FOIA-20180821-6thInterim-Production-pt2.pdf.

[82] *2nd Interim Production: Part 2*, EPIC v. ICE (Palantir Databases), *supra* note 79, at 85-97.

[83] *See* FALCON SEARCH & ANALYSIS SYSTEM 8, DHS/ICE/PIA-032(a) (Jan. 16, 2014), https://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falconsa_january2014.pdf.

[84] *Id.* at 29.

[85] *Id*. at 26-27. The "ENFORCE applications" are used by ICE when arresting people who have violated criminal or immigration laws. ICE employees can access the Enforcement Integrated Database through the ENFORCE applications. PRIVACY IMPACT ASSESSMENT UPDATE FOR THE ENFORCEMENT INTEGRATED DATABASE (EID) 2, DHS/ICE/PIA-015(d) (Apr. 6, 2012), https://www.dhs.gov/sites/default/files/publications/PIA%20EID%20Update%20for%20RCA_EARM%205_CES%202%2020120406%20FINAL%20%5BSigned%5D.pdf.

[86] *4th Interim Production: Part 4*, EPIC v. ICE (Palantir Database), at 1804, https://epic.org/wp-content/uploads/foia/dhs/ice/palantir-databases/EPIC-17-08-14-ICE-FOIA-20180703-4thInterim-Production-pt4.pdf.

[87] *6th Interim Production: Part 1*, EPIC v. ICE (Palantir Databases), at 2544, https://epic.org/wp-content/uploads/foia/dhs/ice/palantir-databases/EPIC-17-08-14-ICE-FOIA-20180821-6thInterim-Production-pt1.pdf.

[88] FALCON SEARCH & ANALYSIS SYSTEM 7, DHS/ICE/PIA-032(b) FALCON-SA (Oct. 11, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice032b-falconsa-appendixbupdate-march2021.pdf.

[89] FALCON SEARCH & ANALYSIS SYSTEM 19, DHS/ICE/PIA-032(a) (Jan. 16, 2014), https://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falconsa_january2014.pdf.

[90] *Id*. at 18.

[91] *Id*. at 18-19.
[92] PRIVACY IMPACT ASSESSMENT FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE (AFI) 4 (June 1, 2012), https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_afi_june_2012_0.pdf.
[93] *Id*. at 9-10.
[94] *Id*. at 10-11.
[95] PRIVACY IMPACT ASSESSMENT UPDATE FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE (AFI) 3, DHS/CBP/PIA-010(a) (Sept. 1, 2016), https://www.dhs.gov/sites/default/files/2022-03/privacy-pia-cbp010%28a%29-afi-march2022.pdf; PRIVACY IMPACT ASSESSMENT FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE (AFI), *supra* note 92, at 3.
[96] 82 Fed. Reg. 44,198, 44,199 (Sept. 21, 2017), https://www.govinfo.gov/content/pkg/FR-2017-09-21/pdf/2017-19718.pdf.
[97] PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM 4 (Aug. 3, 2007), https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats_updated_fr_0.pdf.
[98] *Id*. at 5, 31.
[99] *Id*. at 3.
[100] PRIVACY IMPACT ASSESSMENT UPDATE FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE (AFI) (Sept. 1, 2016), *supra* note 95, at 9.
[101] *Id.* at 7-8.
[102] PRIVACY IMPACT ASSESSMENT FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE (AFI) (June 1, 2012), *supra* note 92, at 6.
[103] *Id*. at 9.
[104] PRIVACY IMPACT ASSESSMENT FOR THE DATA ANALYSIS SYSTEM (DAS) 1, DHS/ICE DAS/PIA-048 (Sept. 19, 2017), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-das-september2017.pdf.
[105] ICE INTELLIGENCE CENTERS: HOW ICE GATHERS DATA TO CONDUCT RAIDS AND DEPORTATIONS 5, JUST FUTURES L. ET AL. (2021), https://www.flipsnack.com/justfutures/ice-intelligence-centers/full-view.html.
[106] PRIVACY IMPACT ASSESSMENT FOR THE DATA ANALYSIS SYSTEM (DAS), *supra* note 104, at 6.
[107] *Id*. at 9.
[108] *Id*. at 9.
[109] *Id*. at 2.
[110] *Id*. at 1.
[111] *Id*. at 3-4.
[112] *Id*. at 9.
[113] *Id*. at 10.
[114] PRIVACY IMPACT ASSESSMENT FOR THE DATA ANALYSIS SYSTEM (DAS), *supra* note 104, at 14-15.
[115] *Id*. at 12.
[116] *Id*. at 9.
[117] *Id.* at 15.
[118] *See* 73 Fed. Reg. 48,226, 48,227 (Aug. 18, 2008), https://www.govinfo.gov/content/pkg/FR-2008-08-18/html/E8-19031.htm.
[119] *See id*.
[120] *See id*. at 48,229.
[121] *See id*.
[122] *See id*.
[123] *See* PRIVACY IMPACT ASSESSMENT FOR ICE INVESTIGATIVE CASE MANAGEMENT, DHS/ICE/PIA-045 (June 17, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf; *id*. at 16; *see also 3rd Interim Production: Part 3*, EPIC v. ICE (Palantir Databases), at 37-48, https://epic.org/wp-content/uploads/foia/dhs/ice/palantir-databases/EPIC-17-08-14-ICE-FOIA-20180521-3rdInterim-Production-pt3.pdf (presentation regarding the modernization of ICE TECS); *3rd Interim Production: Part 4*, EPIC v. ICE (Palantir Databases), at 38, 53-64, https://epic.org/wp-content/uploads/foia/dhs/ice/palantir-databases/EPIC-17-08-14-ICE-FOIA-20180521-3rdInterim-Production-pt4.pdf (same).
[124] *See FOIA CASES: EPIC v. ICE (Palantir Databases)*, supra note 80.
[125] PRIVACY IMPACT ASSESSMENT FOR ICE INVESTIGATIVE CASE MANAGEMENT, *supra* note 36, at 9-12.

[126] *Id*. at 10-11.
[127] *Id*. at 11.
[128] *Id*. at 13.
[129] *Id.* at 1.
[130] *Id*. at 9.
[131] *Id*. at 9-11.
[132] *Id*. at 18.
[133] *Id*. at 28-29.
[134] *Id*. at 30.
[135] PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING (Dec. 22, 2010), https://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf.
[136] PRIVACY IMPACT ASSESSMENT FOR ICE INVESTIGATIVE CASE MANAGEMENT, *supra* note 36, at 16-17.
[137] PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING, *supra* note 135, at 9.
[138] *Id*.
[139] *See Documents Obtained Under Freedom of Information Act: How U.S. Immigration & Customs Enforcement and State Motor Vehicle Departments Share Information*, NAT'L IMMIGR. L. CTR. (May 2016), https://www.nilc.org/issues/drivers-licenses/ice-dmvs-share-information.
[140] *Terrorist Screening Center*, FBI, https://archives.fbi.gov/archives/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/terrorist-screening-center-1.
[141] *See* DAVID LEINS & NARGIS RAHMAN, TRACKED AND TRACED: HOW THOUSANDS OF AMERICAN MUSLIMS ENDED UP ON THE TERRORIST WATCH LIST, PULITZER CTR. (Jan. 20, 2022), https://pulitzercenter.org/stories/tracked-and-traced-how-thousands-american-muslims-ended-terrorist-watch-list.
[142] PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID) 2 (Jan. 14, 2010), https://www.dhs.gov/sites/default/files/publications/PIA%2C%20ICE-EID%2C%2020100118%2C%20%5Bsigned%5D.pdf.
[143] *Id.* at 7-9.
[144] PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING, *supra* note 135, at 14.
[145] PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SURVEILLANCE SYSTEM (ELSUR) 4 (Nov. 2, 2010), https://www.dhs.gov/sites/default/files/publications/privacy_pia_24_ice_elsur.pdf.
[146] *Id.* at 5-6.
[147] *Id*. at 10.
[148] *Id.* at 7.
[149] *Id*. at 11-12.
[150] *Id.* at 10.
[151] 73 Fed. Reg. 9,233, https://www.govinfo.gov/content/pkg/FR-2010-03-01/html/2010-4102.htm.
[152] *Id*. at 9,235.
[153] *Id*.
[154] *Id*.
[155] *Id*. At 9,234.
[156] *Id*.
[157] *See infra* notes 159-164 and accompanying text.
[158] 75 Fed. Reg. 9,233, 9,235 (Mar. 1, 2010), https://www.govinfo.gov/content/pkg/FR-2010-03-01/html/2010-4102.htm.
[159] PRIVACY IMPACT ASSESSMENT FOR THE LAW ENFORCEMENT INTELLIGENCE FUSION SYSTEM (IFS) 9-10 (Nov. 17, 2008), https://www.dhs.gov/sites/default/files/publications/ice-pia-007-IFS-2008.pdf.
[160] *Id*. at 9.
[161] *Id*. at 6.
[162] *Id*. at 5.
[163] 75 Fed. Reg. 9,233, 9,235 (Mar. 1, 2010), https://www.govinfo.gov/content/pkg/FR-2010-03-01/html/2010-4102.htm.

[164] PRIVACY IMPACT ASSESSMENT FOR THE LAW ENFORCEMENT INTELLIGENCE FUSION SYSTEM, *supra* note 159, at 13.
[165] 85 Fed. Reg. 74,362 (Nov. 20, 2020), https://www.govinfo.gov/content/pkg/FR-2020-11-20/pdf/2020-25619.pdf.
[166] *Id.* at 74,364.
[167] *Id*.
[168] *Id*.
[169] *Id*. at 74,365.
[170] *Id*. at 74,363.
[171] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[172] *See* Christiano Lima & Aaron Schaffer, *ICE's Use of Data Brokers to 'Go Around' Sanctuary Laws Under Fire*, WASH. POST. (July 27, 2022), https://www.washingtonpost.com/politics/2022/07/27/ices-use-data-brokers-go-around-sanctuary-laws-under-fire; Johana Bhuiyan, *US Immigration Agency Explores Data Loophole to Obtain Information on Deportation Targets*, GUARDIAN (Apr. 20, 2022), https://www.theguardian.com/us-news/2022/apr/19/us-immigration-agency-data-loophole-information-deportation-targets; Mack DeGeurin, *'This Is a Massive Loophole:' Activists Slam ICE for Using LexisNexis Data to Target Undocumented Immigrants*, GIZMODO (July 27, 2022), https://gizmodo.com/lexisnexis-ice-data-brokers-undocumented-immigrants-1849340046.
[173] S. 1265, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1265.
[174] *See* Press Release, Ron Wyden, Wyden, Paul and Bipartisan Members of Congress Introduce The Fourth Amendment Is Not For Sale Act (Apr. 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-.
[175] *E.g.*, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data*, ACLU (July 18, 2022), https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data.
[176] *See* SYSTEM OF RECORDS NOTICE (SORN) GUIDE 2, OPM (Apr. 2010), https://www.opm.gov/information-management/privacy-policy/privacy-references/sornguide.pdf.
[177] M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 § II(B)(a), at 3, https://www.justice.gov/opcl/page/file/1131721/download.
[178] *See supra* note 17 and accompanying text.
[179] *See supra* notes 18-19 and accompanying text.
[180] *See* STACEY GRAY & POLLYANNA SANDERSON, POLICY BRIEF: LOCATION DATA UNDER EXISTING PRIVACY LAWS 2, FUTURE OF PRIVACY F. (2020), https://fpf.org/wp-content/uploads/2020/12/FPF_Guide_Location_Data_v2.2.pdf.
[181] *See* Privacy Policy Guidance Memorandum 1, Memorandum No. 2008-02, DHS (Dec. 30, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-02.pdf.
[182] *See* THE DEADLY DIGITAL BORDER WALL, MIJENTE, JUST FUTURES L., & NO BORDER WALL COALITION, https://notechforice.com/wp-content/uploads/2021/10/Deadly.Digital.Border.Wall_.pdf; Shirin Ghaffray, *The "Smarter" Wall: How Drones, Sensors, and AI Are Patrolling the Border*, VOX (Feb. 7, 2020), https://www.vox.com/recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai.
[183] See *supra* notes 38-40 and accompanying text.
[184] *See* A BETTER WAY: COMMUNITY-BASED PROGRAMMING AS AN ALTERNATIVE TO IMMIGRANT INCARCERATION, NAT'L IMMIGR. JUST. CTR. (Apr. 22, 2019), https://immigrantjustice.org/research-items/report-better-way-community-based-programming-alternative-immigrant-incarceration#best-practices.

## CHANGE LOG:

[September 12, 2022]:

- Removed references to Palantir that implied the company is a data broker.
- Updated the sections on ICM and FALCON-SA to better reflect the user base of those systems.