GLOSSARY AT A GLANCE

Immigration Databases, Information Sharing Systems, and Case Management Systems

AUGUST 2021

THIS TABLE INTRODUCES THE VOCABULARY used by some federal and state databases and information sharing systems and federal investigative and case management systems and technology that play a role in immigration enforcement. It does not aim to be comprehensive, because the databases and systems are so numerous and the interrelationships among them so complex. Immigration enforcement depends not only on these databases and this technology — informal communications or collaboration between U.S. Immigration and Customs Enforcement (ICE) and state and local law enforcement officers or department of motor vehicle employees also play an important role. We hope this table will help uncover the mystery behind some of these databases and systems, often known only by their acronyms.

A *list of acronyms and abbreviations* used in the table is provided on page 13. For more detailed information, see our report *Untangling the Immigration Enforcement Web: Basic Information for Advocates about Databases and Information Sharing Among Federal, State, and Local Agencies* (www.nilc.org/untangling-immigration-enforcement-web/).

NAME	DESCRIPTION	HYPERLINKS
U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE), and U.S. Customs and Border Protection (CBP) Databases and Information Systems		
Alien Criminal Response Information Management System (ACRIMe)	According to DHS, "The Alien Criminal Response Management Information System (ACRIMe) is an information system used by U.S. Immigration and Customs Enforcement (ICE) to support various law enforcement activities at the ICE Law Enforcement Support Center (LESC) and other ICE locations. ACRIMe supports ICE's handling of a response to immigration status Inquiries made by other agencies regarding individuals arrested, subject to background checks, or otherwise encountered by those agencies. "The system provides real-time immigration status determinations to federal, state, local, tribal, and international criminal justice agencies who submit Immigration Alien Queries (IAQ) to ICE. After receiving an IAQ, ICE uses ACRIMe to research the subject of the IAQ, determine the immigration status of the subject, and generate an Immigration Alien Response (IAR) which is ultimately forwarded to the requesting criminal justice agency."	• https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/daa-0567-2017-0002_sf115.pdf • https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-acrime-september2018.pdf • https://www.regulations.gov/document/DHS-2018-0013-0001

LOS ANGELES (Headquarters)
3450 Wilshire Blvd. #108 – 62
Los Angeles, CA 90010
213 639-3900
213 639-3911 fax

NATIONAL IMMIGRATION LAW CENTER

WASHINGTON, DC
P.O. Box 34573
Washington, DC 20043
202 216-0261
202 216-0266 fax

NAME	DESCRIPTION	HYPERLINKS
	ACRIMe supports the Secure Communities system (see description below). DHS reported in 2010 that it was combining ACRIMe and Enforcement Integrated Database (EID) (see description below) data via the ICE Integrated Decision Support (IIDS) System, a reporting subsystem of EID. In 2018, DHS announced that it was changing the ACRIMe's name to the Criminal History and Immigration Verification (CHIVe) records system, described below.	
Arrival and Departure Information System (ADIS)	According to DHS, "U.S. Customs and Border Protection (CBP) Arrival and Departure Information System (ADIS) consolidates data from a variety of systems to create a unique person-centric record with complete travel history" regardless of citizenship.	• https://www.dhs.gov/sites/default/files/publications/privacy-pia-024c-adis-december2020.pdf
Automated Biometric Identification System (IDENT)	IDENT is a DHS-wide database where biometric information such as fingerprints (taken, e.g., when an individual applies for immigration benefits or is arrested on immigration charges) and associated biographical information are stored and are searchable. DHS is in the processing of replacing IDENT with a database with expanded biometric and other capabilities called Homeland Advanced Recognition Technology (HART), described more fully below.	• https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-06252013_0.pdf • https://www.federalregister.gov/documents/2016/12/15/2016-30187/supplemental-programmatic-environmental-assessment-spea-for-the-proposed-establishment-and • https://www.dhs.gov/sites/default/files/publications/DHS%20Biometrics%20%20Strategic%20Framework%20Webinar%20Slidedeck%20-%20October%2020%202015.pdf
CBP Intelligence Records System (CIRS)	CIRS was announced by DHS/CBP in a Sept. 21, 2017, System of Records Notice (SORN). According to the SORN, "CIRS contains information collected by CBP to support CBP's law enforcement intelligence mission. This information includes raw intelligence information collected by CBP's [Office of Intelligence], public source information, and information initially collected by CBP pursuant to its immigration and customs authorities. This information is analyzed and incorporated into intelligence products. CBP currently uses the Analytical Framework for Intelligence (AFI) and the Intelligence Reporting System (IRS) information technology (IT) systems to facilitate the development of finished intelligence products. These products are disseminated to various stakeholders including CBP executive management, CBP operational units, various government agencies, and the Intelligence Community (IC)." Public sources include "social media, news media	• https://www.federalregister.gov/documents/2017/09/21/2017-19718/privacy-act-of-1974-dhscbp-024-intelligence-records-system-cirs-system-of-records

NAME	DESCRIPTION	HYPERLINKS
	outlets, and the Internet." Government agencies include federal, state, local, as well as foreign agencies.	
Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records	CARIER is an updated and renamed version of DHS/U.S. Immigration and Customs Enforcement (ICE)-011 Immigration and Enforcement Operational Records (ENFORCE) system of records. "This system of records covers records documenting ICE's criminal arrests, and also those documenting most of ICE's immigration enforcement actions, such as the issuance of immigration detainers; the arrests, charging, detention, and removal of aliens for administrative immigration violations; the search for and apprehension of fugitive aliens; and ICE decisions concerning the grant or denial of parole to aliens."	• https://www.govinfo.gov/content/pkg/FR-2016-10-19/pdf/2016-25197.pdf
Criminal History and Immigration Verification (CHIVe)	In 2018, DHS issued a SORN that would change, *inter alia*, ACRIMe's "name to Criminal History and Immigration Verification (CHIVe); add one new category of individuals to include individuals seeking approval from HHS to sponsor an unaccompanied alien child and/or other adult members of the potential sponsor's household; add one new category of records to include biometrics for potential sponsors of an unaccompanied alien child and/or other adult members of the potential sponsor's household; expand a category of records to include screening to verify or ascertain citizenship or immigration status, immigration history, and criminal history for sponsorship of unaccompanied alien children; add a new purpose of the system: To screen individuals to verify or ascertain citizenship or immigration status, immigration history, and criminal history to inform determinations regarding sponsorship of unaccompanied alien children who are in the care and custody of HHS; add a new routine use to describe how the DHS may share information from this system of records with HHS; add a new routine use to describe how the DHS may share information from this system of records with HHS …."	• https://www.govinfo.gov/content/pkg/FR-2018-05-08/pdf/2018-09902.pdf
DHS-Victim Information and Notification Exchange (DHS-VINE)	In April 2017, DHS launched the Victims of Immigration Crime Engagement (VOICE) office within ICE and announced the creation of DHS-VINE, "a free, confidential service that provides crime victims/witnesses, their family members, and victim advocates confidential notification of changes in custody status." DHS-VINElink, the online portal to DHS-VINE, allows users to search for detainees (civil immigration incarceration) or in-state custody (criminal incarceration) and be notified of custody changes. DHS-VINElink builds on a commercially developed victim notification network in the criminal justice system called VINE.	• https://www.dhs.gov/news/2017/04/26/dhs-announces-launch-new-office-victims-illegal-immigrant-crime • https://vinelink.dhs.gov/#/map • https://vinelink.com/#/home

NAME	DESCRIPTION	HYPERLINKS
Enforcement Integrated Database (EID)	EID is a DHS-wide database containing information related to the investigation, arrest, booking, detention, and removal of people encountered during immigration and criminal law enforcement investigations and operations conducted by ICE and CBP.	• https://www.dhs.gov/sites/default/files/publications/privacy_pia%20update_ice_enforcement%20integrated%20database_april%202014.pdf
Homeland Advanced Recognition Technology (HART)	DHS's Homeland Advanced Recognition Technology (HART) is replacing DHS's current IDENT (Automated Biometric Identification System) biometrics database. It will centralize access to federal and international databases, provide real-time access in the field, and involve the use of "multi-modal biometrics" (e.g., the wide range of physical and behavioral characteristics that the NPRM authorizes). DHS disclosed the creation of HART in 2016 and has not issued a SORN that describes its full operation, instead issuing a privacy impact assessment (PIA) in 2020 that describes only the database's first phase. The 2018 notice about the Department of Homeland Security/ALL–041 External Biometric Records (EBR) System of Records makes clear that, in addition to biometrics and associated biographic information, HART will include identifiers for derogatory information, miscellaneous officer comment information, and encounter data. HART, through EBR, will also include "[r]ecords related to the analysis of relationship patterns among individuals and organizations." EBR will allow "DHS to receive, maintain, and disseminate biometric and associated biographic information from non-DHS entities, both foreign and domestic." The Department of Homeland Security/All–043 Enterprise Biometric Administrative Records (EBAR) System of Records (SOR) will allow HART to "link individuals with their encounters, biometrics, records, and other data elements" and to share information with domestic and international agencies. In addition, "HART may use information from publicly available sources, collected according to the data provider's authority."	• Zack Martin, "Homeland Security Releases Biometric Framework," *Secure ID News*, Aug. 31, 2015, https://www.secureidnews.com/news-item/homeland-security-releases-biometric-framework/. • *Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA* (U.S. Dept. of Homeland Security, DHS/OBIM/PIA-004, Feb. 24, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf • Privacy Act of 1974; System of Records, 83 Fed. Reg. 17829–33 (Apr. 24, 2018), https://www.govinfo.gov/content/pkg/FR-2018-04-24/pdf/2018-08453.pdf. • Privacy Act of 1974; System of Records, 85 Fed. Reg. 14955–58 (Mar. 16, 2020), https://www.govinfo.gov/content/pkg/FR-2020-03-16/pdf/2020-04979.pdf. • Privacy Act of 1974; System of Records, 83 Fed. Reg. 36950–55 (July 31, 2018), https://www.govinfo.gov/content/pkg/FR-2018-07-31/pdf/2018-16138.pdf.
ICEGangs	ICEGangs is an ICE database that serves as a repository of personal information about suspected or confirmed gang members and "associates," as well as information on gang activities. ICE reportedly stopped using ICEGangs in 2016, because ICE agents were relying on other case management databases. ICE has not publicly announced this.	• https://www.ilrc.org/sites/default/files/resources/ilrc_gang_advisory-20170426.pdf

NAME	DESCRIPTION	HYPERLINKS
LeadTrac	According to DHS, "LeadTrac is a database owned by the [HSI] Counterterrorism and Criminal Exploitation Unit (CTCEU). The function of LeadTrac is to vet and manage leads pertaining to visitors in the United States who are suspected of overstaying their period of admission or otherwise violating the terms of their admission, as well as organizations suspected of immigration violations." Suspected status violators are referred to ICE field offices for investigation and enforcement. Information regarding NSEERS is maintained in LeadTrac.	• https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-leadtrac-july2016.pdf, p. 1 • https://www.regulations.gov/document?D=DHS-2016-0053-0001
TECS	According to CBP, "TECS is an information-sharing platform, which allows users to access different databases that may be maintained on the platform or accessed through the platform, and the name of a system of records that include temporary and permanent enforcement, inspection, and operational records relevant to the anti-terrorism and law enforcement mission of CBP and numerous other federal agencies that it supports. TECS not only provides a platform for interaction between these databases and defined TECS users, but also serves as a data repository to support law enforcement 'lookouts,' border screening, and reporting for CBP's primary and secondary inspection processes."	• https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-sar-update_0.pdf
DHS, ICE, and CBP Investigative and Case Management Systems		
Analytical Framework for Intelligence (AFI)	AFI is a CBP system that "provides enhanced search and analytical capabilities to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS at the border." According to a 2016 Privacy Impact Assessment (PIA), AFI incorporates records from other CBP and DHS systems (including the National Security Entry Exit Registration System, or NSEERS) and has now added ICE and local law enforcement data sources, including providing access to the Law Enforcement Information Sharing Services (LEISS). According to the technology-focused website *The Verge*, "the system draws from a variety of federal, state, and local law enforcement databases that gather and analyze often-sensitive details about people, including biographical information, personal associations, travel itineraries, immigration records, and home and work addresses, as well as fingerprints, scars, tattoos, and other physical traits." *The Verge* also reports that AFI no longer just allows access to other databases, but has instead become its own database, copying information it has obtained from other databases onto its servers.	• https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_afi_june_2012_0.pdf • https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-010-a-afi-2016.pdf • https://www.theverge.com/2016/12/21/14012534/palantir-peter-thiel-trump-immigrant-extreme-vetting

NAME	DESCRIPTION	HYPERLINKS
Analytical Records	According to DHS, the DHS/ICE-018 Analytical Records system consolidates two existing systems of records: DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) and DHS/ICE-016 FALCON Search and Analysis (FALCON-SA) (described below). In fact, the Analytical Records SORN expands the categories of individuals covered by FALCON-SA, the records to be included in the system, and the uses and sharing of data from within and outside of the system. Analytical Records is both a database and an analytic tool. With it, ICE "ingests and aggregates" vast quantities of personal information from domestic, international, public, and commercial sources. The range of personal information covers, *inter alia*, biographic information (including Social Security numbers and Individual Taxpayer Identification Numbers); biometrics (including "facial images, iris images, fingerprints, and voice audio"); financial data; location-related data (including addresses, geotags, and geolocation information derived from law enforcement activities, ICE-owned devices, witness accounts or commercially available data); open-source information from the internet, the dark web and social media; data from commercial enterprises; information from law enforcement and foreign governments; investigative leads; and tips submitted to ICE. The information collected involves not only the subjects of an investigation or incident, but also witnesses or persons "associated with" incidents or "suspicious activities." The system's "data store" will ingest information from other government data systems on a regular basis. It will also ingest information on an ad hoc basis from "commercial or public sources (e.g., internet research or from a commercial data service), public reports of law enforcement violations or suspicious activity (tips), or digital records seized or subpoenaed during an investigation." It will also contain "metadata that is created by an ICE analytical system when it ingests data" that will provide "contextual information." ICE's analytical systems "also ingest external information from nonfederal entities, including state and local law enforcement authorities, private corporations, or foreign governments." The external information could include "biographic information, trade and customs information, criminal history information, content from the dark net, and publicly available social media content," and potentially much more. Analytical Records uses "indexes to conduct searches, identify relationships and links between records and data, and generate visualizations for analytic purposes." In addition, "Users of an analytical tool or system may create visualizations, match records, or create analyses of large volumes of data through algorithmic processes."	• Notice of a New Privacy Act System of Records: "DHS/ICE–018 Analytical Records'' Docket Number ICEB–2020–0008, (March 22, 2021), https://www.govinfo.gov/content/pkg/FR-2021-03-22/pdf/2021-05651.pdf.

NAME	DESCRIPTION	HYPERLINKS
FALCON	FALCON is an information technology platform developed by the private company Palantir. It has several components: • FALCON Search & Analysis (FALCON-SA) • FALCON Tip Line (FALCON-TL) • FALCON Data Analysis & Research for Trade Transparency System (FALCON-DARTTS) • FALCON Roadrunner According to a notice of Privacy Act exemptions, "In 2012, ICE HSI created a new IT environment called 'FALCON' to support ICE's law enforcement and criminal investigative missions. The FALCON environment is designed to permit ICE law enforcement and homeland security personnel to search and analyze data ingested from other Government [sic] applications and systems while employing appropriate user access restrictions at the data element level and robust user auditing controls." FALCON-SA and FALCON-TL are described in more detail below.	• https://www.gpo.gov/fdsys/pkg/FR-2017-05-04/html/2017-09026.htm
FALCON Search and Analysis (FALCON-SA)	Falcon-SA is a "consolidated information management system that enables ICE law enforcement and homeland security personnel to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws." FALCON-SA routinely ingests and allows users to query information from all the FALCON components, ICM, the Immigration and Enforcement Operational Records System (ENFORCE) — which includes ICE, CBP, and U.S. Citizenship and Immigration Services (USCIS) arrest and investigation records — and other ICE systems. On an ad hoc basis, FALCON-SA includes commercially available or public source data, criminal history information (including data from NCIC and state and local law enforcement), foreign government information, and more.	• https://www.gpo.gov/fdsys/pkg/FR-2017-05-04/html/2017-09026.htm • https://www.dhs.gov/publication/dhsicepia-032a-falcon-search-analysis-system-falcon
FALCON Tip Line (FALCON-TL)	According to a 2012 DHS/ICE PIA, FALCON-TL is a "workflow management system [that] supports the creation and maintenance of tips received by the HSI Tipline Unit about suspicious activity or suspected illegal activity, and the referral of this information to HSI field offices for appropriate investigation or other follow up." The public and state and local law enforcement can submit tips via an online form or by phone. Once a tip is found to be "actionable," it goes into FALCON-SA.	• https://www.dhs.gov/sites/default/files/publications/ice-pia-033-falcon-tipline-2012.pdf

NAME	DESCRIPTION	HYPERLINKS
ICE Pattern Analysis and Information Collection (ICEPIC)	According to a 2008 PIA, "ICEPIC is a set of information analysis tools which allow disparate sources of information to be analyzed to find previously unknown relationship data about individuals who are the subject of ongoing and valid investigations. Relationship data is made up of information about how a place, person, or thing (e.g., automobile or other piece of property) relates to other persons, places, or things." According to a 2011 PIA, "ICEPIC data is accessed by external federal, state, local, tribal and international law enforcement agency partners (member agencies) through a web service called the LEIS Service. The member agencies use the LEIS Service as a sharing service to access filtered information from ICEPIC." A 2016 PIA regarding ICM said ICEPIC would be retired in 2016. It's not clear if it has been.	• https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_icepic-4a.pdf • https://www.gpo.gov/fdsys/pkg/FR-2008-08-18/html/E8-19031.htm • https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-pic-january2008.pdf • https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf, p. 29
Intelligence Reporting System (IRS)	The Intelligence Reporting System is referred to in several CBP documents but not defined. A 2017 PIA for the Intelligence Records System says that IRS and AFI technology systems are used "to facilitate the development of finished intelligence products." The PIA reports that a PIA for IRS is forthcoming. It appears to have been in existence for some time, as it is referred to in a 2012 PIA for the Automated Targeting System.	• https://www.federalregister.gov/documents/2017/09/21/2017-19718/privacy-act-of-1974-dhscbp-024-intelligence-records-system-cirs-system-of-records • https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf
Investigative Case Management (ICM)	ICM is an information technology system/law enforcement management tool developed by the private company Palantir. It is used primarily by ICE Homeland Security Investigations (HSI) for criminal and civil prosecutions and investigations. ICE Enforcement and Removal Operations (ERO) can use ICM to manage criminal immigration cases and to query the system for information supporting civil cases. ICM allows ICE personnel to "create an electronic case file that organizes and links all records and documents associated with a particular investigation so they are easily accessible from a single location. It also enables personnel to link records to multiple investigations in order to draw connections between cases …."	• https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/
Law Enforcement Information Sharing Service (LEISS, sometimes abbreviated as LEIS)	According to DHS, "The Law Enforcement Information Sharing Service is a web-based data exchange platform, hosted by [DHS], that allows law enforcement agencies to rapidly share and access data related to criminal and national security investigations. … "DHS law enforcement information is processed through the ICE Pattern Analysis and Information Collection System [hyperlink omitted] and includes information from subject records and closed cases concerning people, businesses, vehicles (including aircraft and seacraft [sic]), firearms and more.	• https://www.ice.gov/le-information-sharing

NAME	DESCRIPTION	HYPERLINKS
	"The Law Enforcement Information Sharing Service currently provides federal, state, local, tribal and international law enforcement agency partners with access to more than 2.6 million subject records related to persons of interest, including suspects in child pornography, drug smuggling, immigration fraud, alien smuggling and a wide range of other cases." DHS reports on its website that it has deployed the service "on a regional basis in San Diego, Los Angeles, Seattle, Arizona, and Texas. In addition, the U.S. Department of Justice established connectivity to the service via the OneDOJ program" [hyperlink omitted].	
U.S. Department of Justice (DOJ) Databases		
Interstate Identification Index (III)	Per 28 CFR 20.3(m), the Interstate Identification Index system, or III system, is "the cooperative federal-state system for the exchange of criminal history records, and includes the National Identification Index, the National Fingerprint File, and, to the extent of their participation in such system, the criminal history record repositories of the states and the FBI." The III system is maintained by the Federal Bureau of Investigation.	• https://www.law.cornell.edu/cfr/text/28/20.3. See https://www.fbi.gov/file-repository/interstate-identification-index-iii-national-fingerprint-file-nff.pdf/view for participating states.
National Crime Information Center (NCIC)	NCIC is an FBI database containing "an electronic clearinghouse of crime data that can be tapped into by virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year." Despite the FBI's description of the NCIC as a criminal database, it also contains civil immigration information, such as information regarding persons with outstanding immigration removal orders and persons designated as "criminal aliens" who have been deported. It also includes a Gang File.	• https://fas.org/irp/agency/doj/fbi/is/ncic.htm
National Data Exchange (N-DEx)	N-DEx is an "unclassified national information sharing system that enables criminal justice agencies to search, link, analyze, and share local, state, tribal, and federal records. N-DEx is also a strategic investigative information sharing system that fills informational gaps and provides situational awareness." N-DEx and many regional and state data exchanges have information sharing agreements with ICE.	• https://www.fbi.gov/services/cjis/ndex • https://justfutureslaw.org/statedmvtech/
Next Generation Identification (NGI)	NGI is an expanded FBI biometric database (including fingerprints, iris prints, palm prints) with advanced services, including a facial recognition system and ongoing status notification of criminal history. It replaces the Integrated Automated Fingerprint Identification System (IAFIS). NGI also offers services such as the Repository for Individuals of Special Concern (RISC), which allows law enforcement to take fingerprints in the field using mobile devices and	• https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi • https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/iafis-ngi-risc

NAME	DESCRIPTION	HYPERLINKS
	to check them against the NGI databases, getting responses in a matter of seconds. The NCIC's Immigration Violator File can be checked through the RISC.	• https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi
Interoperability Between DOJ and DHS Databases		
Secure Communities (S-Comm)	Under S-Comm, a fingerprint check of arrested persons against FBI databases results in an automated check (interoperability) against DHS databases. The system notifies ICE when there is a "hit," and ICE then determines whether to take enforcement action against the individual arrested.	• https://www.ice.gov/secure-communities
State and Commercial Databases and Information Sharing Systems		
Accurint	According to its owner, LexisNexis, "Accurint® for Law Enforcement is a cutting-edge investigative technology that can expedite the identification of people and their assets, addresses, relatives and business associates by providing instant access to a comprehensive database of public records that would ordinarily take days to collect." In Feb. 2021, LexisNexis entered into a contract with ICE. "The contract shows LexisNexis will provide Homeland Security investigators access to billions of different records containing personal data aggregated from a wide array of public and private sources, including credit history, bankruptcy records, license plate images, and cellular subscriber information. "	• https://risk.lexisnexis.com/products/accurint-for-law-enforcement • https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/ • https://www.flipsnack.com/JustFutures/commercial-and-utility-data-report/full-view.html
Clearview AI	Clearview AI is an American company that created a facial recognition technology which is used by ICE and CBP, as well as many other law enforcement agencies. According to its website, it is a "facial recognition search engine with over 3 billion images sourced from the public internet, including news media, mugshot websites, public social media, and many other open websites."	• https://clearview.ai • https://thehill.com/policy/technology/548932-pressure-mounts-on-dhs-to-stop-using-clearview-ai-facial-recognition
Consolidated Lead Evaluation and Reporting database (CLEAR)	The CLEAR database is owned by Thomson Reuters. According to a Thomson Reuters shareholders resolution, "CLEAR consolidates public records across numerous databases, such as motor vehicle and arrest records, utilities, health care provider information, cellphone records, and license plate recognition." ICE uses CLEAR to track people whom it considers to be undocumented.	• Kim Lyons, "Thomson Reuters Faces Pressure Over ICE Contracts, *The Verge*, May 21, 2020, https://www.theverge.com/2020/5/21/21266431/thomson-reuters-ice-clear-software. • McKenzie Funk, "How ICE Picks Its Targets in the Surveillance Age," *New York Times Magazine*, Oct. 3, 2019,

NAME	DESCRIPTION	HYPERLINKS
		https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.
COPLINK	COPLINK, owned by Forensics Logic, is a "data sharing and crime analytics platform." According to a 2018 report, "Using COPLINK, law enforcement can search through enormous amounts of data on people, some of whom have contact with police but no convictions. Police can search race, hair color, eye color, complexion, ethnicity, country of origin, and even tattoos and other distinguishing marks on their bodies. Once selected, law enforcement can sort and display a person's [']associational data,[']information on other people connected with the person, with the option to literally map out the person's life by showing their network of friends and associates, vehicles, and organizations." COPLINK has been integrated with Thomson Reuters Consolidated Lead Evaluation and Reporting database (CLEAR) used by ICE in immigration enforcement.	• https://forensiclogic.com • https://gizmodo.com/how-ice-is-gaining-a-scary-amount-of-data-through-polic-1825613345 • https://www.nilc.org/wp-content/uploads/2020/11/Nlets-Q-and-A.pdf
GangNet	GangNet is a commercial intranet-linked software that offers a database with information and photos on individuals and gangs, data analysis, facial recognition software, mapping, a field interview form, and a watch list. Using a single command, agencies can simultaneously search their own GangNet system and a network of GangNet systems in other states and federal agencies. The GangNet software is operational in many states (Arizona, California, District of Columbia, Florida, Georgia, Maryland, Minnesota, Nevada, New Mexico, North Carolina, South Carolina, Texas, Virginia, Washington), as well as in Canada. ICE, the FBI, and the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) are also connected to it and able to share information in real time.	• http://www.law.uci.edu/academics/real-life-learning/clinics/ucilaw-irc-MislabeledReport.pdf • https://assets.documentcloud.org/documents/1683801/gangnet8-whitepaper2013.pdf
Nlets	Nlets is a state-owned telecommunications network and describes itself as "the premiere interstate justice and public safety network in the nation for the exchange of law enforcement-, criminal justice-, and public safety–related information." It is used by criminal justice agencies in U.S. states and territories, federal criminal justice agencies including ICE, and some international agencies. Data that can be exchanged through Nlets includes criminal histories, motor vehicles and driver's license and driving history data, and much more. Currently many states share driver's license photos through Nlets.	• http://www.nlets.org/about/who-we-are • See http://www.nlets.org/our-members/grantmaps?mapid=d26b4e70-934e-11e3-9a61-00155d003202 for driver's license photo-sharing map • https://www.nilc.org/issues/immigration-enforcement/nlets-questions-and-answers/
Vigilant Solutions	Vigilant Solutions, owned by Motorola, is a widely used automated license plate reader service (ALPR). Through services like Vigilant Solutions, ICE has access to license plate scans by fixed and mobile cameras operated by law enforcement agencies and private companies. Vigilant data is available to ICE through CLEAR, described above.	• https://www.vigilantsolutions.com/page/2/ • https://www.aclunc.org/blog/records-reveal-ice-agents-run-thousands-license-

NAME	DESCRIPTION	HYPERLINKS
		plate-queries-month-massive-location-database • https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html
State criminal justice databases	States have their own criminal justice networks that collect and share information related to their criminal justice systems and their departments of motor vehicles (DMVs). For example, in Connecticut, the Connecticut On-Line Law Enforcement Communications Teleprocessing (COLLECT) system includes state criminal history and DMV records as well as other state databases, and provides access to databases in other states as well as databases administered by the U.S. and Canada through Nlets and NCIC.	• http://www.ct.gov/cjis/cwp/view.asp?a=4103&q=480592
State department of motor vehicles (DMV) databases	Though state DMV databases differ from state to state, in general they contain information provided in obtaining a driver's license or that appears on the face of a license, driver's license photographs, car registration information, car insurance information, and traffic offense information. ICE obtains information in state DMV databases through Nlets, state criminal justice databases, and informal communications between ICE and DMV employees.	• www.nilc.org/ice-dmvs-share-information/ • https://justfutureslaw.org/statedmvtech/
State-to-State Verification Service	6 CFR sec. 37.29 requires states to check with all other states to ensure that a driver holds only one driver's license and only one REAL ID credential (whether a driver's license or an identification card). The American Association of Motor Vehicle Administrators (AAMVA), a non-profit that represents the state, provincial, and territorial officials in the United States and Canada who administer and enforce motor vehicle laws, developed the State-to-State (S2S) Verification Service to comply with these requirements. The platform that supports S2S is called the State Pointer Exchange Services (SPEXS). The S2S information exchange system includes a central database which contains personal information about drivers, including the last five digits of their Social Security numbers and whether they have a REAL ID–compliant license.	• 6 CFR § 37.29, https://www.law.cornell.edu/cfr/text/6/37.29. • "State-to-State (S2S) Verification Services" (American Association of Motor Vehicle Administrators webpage), https://www.aamva.org/State-to-State/.

ACRONYMS & ABBREVIATIONS USED IN THE TABLE

ACRIMe – Alien Criminal Response Information Management System

ADIS – Arrival and Departure Information System

AFI – Analytical Framework for Intelligence

ATF – U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives

CBP – U.S. Customs and Border Protection

CIRS – CBP Intelligence Records System

COLLECT – Connecticut On-Line Law Enforcement Communications Teleprocessing

CARIER – Criminal Arrest Records and Immigration Enforcement Records

CHIVe – Criminal History and Immigration Verification

CLEAR – Consolidated Lead Evaluation and Reporting

CTCEU – HSI Counterterrorism and Criminal Exploitation Unit

DHS – U.S. Department of Homeland Security

DHS-VINE – DHS-Victim Information and Notification Exchange

DMV – department of motor vehicles

DOJ – U.S. Department of Justice

EID – Enforcement Integrated Database

ENFORCE – Immigration and Enforcement Operational Records System

ERO – ICE Enforcement and Removal Operations

FALCON-DARTTS – FALCON Data Analysis & Research for Trade Transparency System

FALCON-SA – FALCON Search & Analysis

FALCON-TL – FALCON Tip Line

FBI – Federal Bureau of Investigation

HART – Homeland Advanced Recognition Technology

HSI – ICE Homeland Security Investigations

IAFIS – Integrated Automated Fingerprint Identification System

ICE – U.S. Immigration and Customs Enforcement

ICEPIC – ICE Pattern Analysis and Information Collection

ICM – Investigative Case Management

IDENT – Automated Biometric Identification System

III – Interstate Identification Index

IRS – Intelligence Reporting System

IT – information technology

LEIS – See LEISS

LEISS – Law Enforcement Information Sharing Services (sometimes referred to as LEIS)

NCIC – National Crime Information Center

N-DEx – National Data Exchange

NGI – Next Generation Identification

NSEERS – National Security Entry Exit Registration System

PIA – Privacy Impact Assessment

RISC – Repository for Individuals of Special Concern

S-Comm – Secure Communities

SORN – System of Records Notice

S2S – State-to-State Verification Service

TECS [not an acronym]

USCIS – U.S. Citizenship and Immigration Services

VOICE – Victims of Immigration Crime Engagement