



The Expansion of AI-Driven Biometric Systems in Immigration Enforcement

Introduction

U.S. Immigration and Customs Enforcement (ICE) is increasingly relying upon an extensive biometric data¹ and artificial intelligence (AI)² infrastructure in conducting operations. What began as a modest set of legacy identification tools has grown, through a rapid sequence of contracts and pilot programs between 2025 and 2026, into an interconnected system spanning facial recognition, iris scanning, real-time field surveillance, and AI-assisted targeting. In a short period, the population touched by this infrastructure has widened considerably. It now extends from individuals in active removal proceedings, to their family members and neighbors whose addresses appear in the same records, to protesters photographed at demonstrations, to the roughly one-third of American adults whose driver's license photos are searchable by federal agents through existing data-sharing networks. This expansion is not simply a matter of more tools doing the same job faster. As this paper details, AI-driven platforms like ImmigrationOS and ELITE consolidate case data, government records, and biometric identifiers that previously existed in separate systems into single, continuously updated profiles, extending well beyond the population of noncitizens with pending immigration matters. At the same time, federal laws and regulations are limited in addressing how these AI tools collect, retain, or share this data, leaving agencies substantial discretion over deployment even as they touch citizens and noncitizens alike.

This paper traces that expansion in four parts. It first describes the legacy biometric and case-management infrastructure that predates the current AI buildout, including DHS's

¹ “A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.” National Institute of Standards and Technology, “Biometrics,” Computer Security Resource Center, accessed July 21, 2026, <https://csrc.nist.gov/glossary/term/biometrics>

² “An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.” Organisation for Economic Co-operation and Development (OECD), Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/o449), adopted May 22, 2019, revised 2023, “Explanatory memorandum on the updated OECD definition of an AI system,” https://www.oecd.org/en/publications/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en.html

Homeland Advanced Recognition Technology (HART) database and ICE's longstanding use of state driver's license records. It then examines three tools introduced or expanded since 2025: ImmigrationOS, a case-management and targeting platform; Mobile Fortify, ICE's field-deployed facial recognition app; and ELITE, a related targeting tool built on public-benefits and government address data. Finally, it considers what this buildout means for individuals well outside ICE's traditional enforcement population and examines the legal and regulatory gaps that currently leave these systems largely self-governed by the agencies that operate them.

Legacy Biometric Infrastructure

Before the recent expansion of AI-driven tools, the Department of Homeland Security (DHS) had already built a substantial biometric infrastructure to support identification and case management across its component agencies. Between 2008 and 2021, ICE [spent](#) nearly \$3 billion to expand surveillance, data collection, and data-sharing initiatives. DHS's Automated Biometric Identification System ([IDENT](#)), which was first [developed](#) in 1994, holds face, iris, fingerprint, and DNA records on more than [320 million](#) people. Many DHS agencies also [rely](#) heavily on the Investigative Case Management (ICM) system, which ICE has used since [2014](#) to organize records, track investigations, and support enforcement operations. ICM has served as the backbone for various ICE activities over the past decade, notably including prior enforcement operations. Additionally, the [Homeland Advanced Recognition Technology](#) (HART) system, [developed](#) in 2015, serves as a central database linking iris scans, fingerprints, and facial images, allowing different DHS components—including ICE, CBP, and USCIS—to query the same biometric profiles for identity verification.

DHS's biometric infrastructure supports immigration enforcement by helping officers establish a person's identity, identify the use of aliases, and connect an individual to relevant immigration and criminal records. For example, IDENT can alert officers when the same fingerprints are associated with different identities or when a person has previously been ordered removed, allowing ICE to pursue enforcement actions based on a more complete and accurate record. DHS has also used this biometric infrastructure for purposes beyond immigration enforcement. During the 2021 evacuation from Afghanistan, authorities [checked](#) evacuees' fingerprints against IDENT and other federal records to verify identities and identify potential security concerns. By the end of fiscal year 2021, USCIS had submitted more than 8,400 biometric records to IDENT through the Afghan Special Immigrant Visa process.

Facial Recognition

[Facial recognition](#) capabilities also predate the current AI buildout. Research has [documented](#) ICE's longstanding use of state driver's license databases for facial recognition searches, a practice that draws on records collected for licensing purposes

rather than law enforcement or immigration matters. Each state's department of motor vehicles (DMV) independently maintains its own driver's license and ID records, including photos, addresses, and physical descriptors. States are not automatically required to give federal agencies like DHS or ICE direct access to this data, and some states, like New York, have laws specifically [blocking](#) such sharing, but the REAL ID Act does require states to make certain license and ID data electronically accessible to other states through a shared verification network.

In practice, most states share DMV data through [Nlets](#), an information exchange “switchboard” originally established in 1967 as the National Law Enforcement Telecommunications System. Nlets is a self-funded, nonprofit corporation governed by state law enforcement agencies that [gives](#) roughly 18,000 federal, state, local, tribal, and territorial law enforcement agencies real-time query access to all 50 states' DMV records. Individual states [retain](#) some control over what they share and with whom, but, absent state-level restrictions, the data is generally available to any Nlets-connected agency without additional court authorization. Police or immigration enforcement officers can compare a person's photo collected in the field against DMV images obtained through Nlets, allowing agents to identify someone even without an independent tip or an existing record. DMV databases are of particular value to ICE because [some states](#) allow residents to obtain a driver's license regardless of immigration status. DHS and its component agencies are able to [access](#) Nlets as an authorized federal member for [criminal justice](#) purposes.

In an Nlets search, a single query is automatically routed to all states that permit multistate connections, and Nlets consolidates their responses into a single reply. The reply can include a driver's name, address, date of birth, physical description, Social Security number, license type, restrictions, license status, and license number, and—where the responding state permits it—a photo. While ICE cannot use a Nlets query to directly flag someone as undocumented, it can be used to confirm the identity of someone already under investigation. Agents can use Nlets to identify individuals based on DMV photos or addresses, their license plates, or photographs of people's faces taken in the field, checking Nlets to locate matches of known license holders. Because of the “switchboard” design, ICE [cannot](#) use Nlets to pull the records of everyone who obtained a license without proof of immigration status. Nlets queries must contain individualized information, so ICE can make a targeted request using an individual's name, date of birth, and sex, or a license number. In the twelve months ending October 2025, ICE alone [submitted](#) more than 292,000 queries through Nlets.

ImmigrationOS

Building on these legacy systems, the second Trump administration has accelerated the adoption of AI-enabled technologies for immigration enforcement. In April 2025, ICE contracted with a technology firm to build the “Immigration Lifecycle Operating

System,” known as [ImmigrationOS](#), a software platform that ICE agents use to look up information on individuals and generate lists of enforcement targets. ImmigrationOS functions as an analytical layer sitting on top of ICE's existing records, using algorithms to sort through that data and surface individuals or patterns that match criteria set by ICE. According to government documents, the platform was [designed](#) around three functions: 1) targeting and prioritization, 2) self-deportation tracking, and 3) immigration lifecycle management.

The targeting and prioritization function cross-references records to generate ranked lists of individuals ICE should prioritize for arrest. ImmigrationOS [uses](#) AI to sift through immigration records, criminal histories, known affiliations, and prior infractions. Government documents [have asserted](#) that “violent criminals” and people who have overstayed a visa are priority categories, although the agency has not disclosed the specific weighting or thresholds the algorithm uses to rank one person above another. The self-deportation tracking function [monitors](#) travel, reportedly using passport records among other data, to flag when someone appears to have left the country voluntarily. This gives ICE near real-time visibility into compliance without requiring a formal removal order. The immigration lifecycle management function is designed to streamline the deportation process from initial identification through eventual removal, consolidating case data that previously may have existed in separate files into one continuously updated profile.

Of note, the lifecycle function draws on DHS’s existing ICM platform, which ICE and HSI have historically [used](#) for civil and criminal enforcement matters. ICM documentation [notes](#) that U.S. citizens remain subject to criminal prosecution and are therefore included in the system, indicating that its case coverage extends beyond noncitizens in civil immigration proceedings. Public reporting has not confirmed whether Executive Office for Immigration Review (EOIR) immigration court records are directly integrated into the ICM platform. Sources that have been confirmed are considerably broader, [including](#) passport and travel records, Social Security and IRS data, FBI, DEA, ATF, and SEVIS records, HHS and USCIS files, license plate reader data, and commercial data broker products such as CLEAR. Rather than requiring an ICE agent to manually search each of these separate databases one at a time, the system runs combined queries across these databases and then applies machine-learning models to reconcile mismatched identity records and flag individuals meeting enforcement or risk criteria. A working prototype was [expected](#) by September 2025, with the overall contract term running through September 2027. DHS officials [confirmed](#) they had started using the system in January 2026.

Mobile Fortify

ICE initially launched a mobile application called [Mobile Fortify](#) in spring 2025. The application allows authorized ICE agents and certain CBP officers to submit facial

images, fingerprints, and photographs of identity documents from government-issued smartphones for comparison against biometric and immigration records maintained by DHS. Facial images are [routed](#) through CBP's Traveler Verification Service, while fingerprints can be checked against IDENT through the Automated Targeting System. When the system identifies a potential match, it may return limited biographical and immigration information, such as a name, date of birth, citizenship status, alien registration number, previous immigration encounters, or possible visa-overstay status. DHS [presents](#) Mobile Fortify as a tool for improving the speed and accuracy of identity and immigration-status checks during enforcement operations. Mobile biometric matching can help officers quickly generate an identity lead when a person lacks identification, presents potentially unreliable documents, uses an alias, or cannot otherwise be identified through biographical information alone. Previously, officers might have needed to transport a person to an ICE facility for fingerprinting and additional record checks. By making an initial comparison available in the field, Mobile Fortify could reduce those delays, help officers connect a person to an existing immigration record, and potentially avoid prolonged detention when subsequent verification shows that the person encountered is not the intended target. DHS [describes](#) the application as a lawful enforcement tool that queries limited CBP immigration datasets and operates with a deliberately high threshold for confirming a match.

At the same time, DHS does not represent a Mobile Fortify facial-recognition result as conclusive proof of identity. In its [AI Use Case Inventory](#), DHS acknowledges that even a facial-matching algorithm that has performed well in National Institute of Standards and Technology testing may return an incorrect candidate. DHS standard operating procedures and required training instruct officers to treat results only as potential matches, prohibit using a match as the sole basis for enforcement action, and require confirmation through established identity-verification procedures. These safeguards are important because they recognize the technology's proper role as a lead-generation and decision-support tool, rather than a substitute for an officer's investigation or independent evidence.

Nevertheless, questions remain about whether Mobile Fortify is being used in the field consistently with those stated limitations. Facial-recognition systems perform [less reliably](#) when photographs are captured under uncontrolled conditions involving poor lighting, motion, or unusual camera angles. Unlike fingerprints, a facial-recognition result generally identifies a possible candidate rather than establishing a definitive identity.

Despite DHS's stated safeguards, privacy advocates have raised concerns about whose photographs Mobile Fortify may collect, how long the government retains them, and whether records of people who are not subject to immigration enforcement are

subsequently deleted. DHS's [Privacy Threshold Analysis](#) states that ICE does not provide individuals an opportunity to decline or consent to the collection and use of their photographs. It also acknowledges that officers could photograph someone who is not removable, including a U.S. citizen or lawful permanent resident. CBP may retain photographs submitted through the application for as long as 15 years, including photographs that do not produce a correct match, and information shared with another agency may be subject to that agency's separate retention rules. Critics therefore [argue](#) that the tool could create lasting biometric records of citizens, lawful permanent residents, protesters, observers, and other people who are not ultimately shown to be subject to immigration enforcement.

Reported [errors](#) in Mobile Fortify's deployment also raise questions about whether field practices conform to DHS's requirement for independent confirmation. In one documented Oregon case, two photographs of the same detained woman [returned](#) different candidate identities, and the agent testified that the application did not display a confidence score. In another incident, ICE [detained](#) a U.S. citizen after Mobile Fortify associated him with a noncitizen record and released him only after additional investigation. These incidents do not establish the application's overall accuracy, but they illustrate the importance of treating facial-recognition results as investigative leads that require corroboration rather than as definitive identifications.

Separate concerns involve the privacy review completed before Mobile Fortify's deployment. ICE and CBP deployed the application without publishing a PIA specifically addressing Mobile Fortify, even though DHS classified it as a "high-impact" use in its [AI Use Case Inventory](#). The application's [Privacy Threshold Analysis](#) concluded that the program was privacy-sensitive and required PIA and System of Records Notice coverage. ICE and CBP privacy officers nevertheless determined that existing documentation was sufficient, but critics [contend](#) that these earlier documents do not adequately assess the distinct privacy risks created by collecting facial images through a mobile application during interior enforcement encounters.

ELITE

As ImmigrationOS moved toward its September prototype deadline, a company supplier for ICE simultaneously [built](#) a related, but distinct, AI-based targeting tool known as Enhanced Leads Identification & Targeting for Enforcement (ELITE). According to court testimony and internal reporting, ELITE populates a map with potential deportation targets, generates a dossier on each individual, and assigns a "confidence score" reflecting the likelihood that a given address is accurate and current. As one ICE officer [testified](#) in court, the tool "tells you how many people are living in this area and what's the likelihood of them actually being there," allowing agents to identify not just a single target but a cluster of people at a given location whom ICE may wish to target.

The tool [searches](#) address data from a range of government sources, including the Department of Health and Human Services (HHS) and USCIS, to “improve capabilities for identifying and prioritizing high-value targets through advanced analytics,” [according](#) to an ICE internal user guide. In practice, the HHS data at issue is drawn from Medicaid enrollment records, which include home addresses, dates of birth, and immigration status, and which ICE has used specifically to locate where a targeted individual is likely living, rather than to independently identify new targets on the basis of health information itself. ELITE's use became public through court testimony in Oregon, where law enforcement agents [described](#) relying on the tool during a field enforcement operation to identify addresses where multiple people have had “contact with immigration officials, which could include a naturalized US citizen.” In some instances, addresses that individuals had [provided](#) to enroll in Medicaid were used to locate them for enforcement purposes.

Privacy advocates raised [concerns](#) that the system's reliance on Medicaid and other public-benefits data represents a secondary use that health and social-service data were never intended for: Individuals share this information specifically to obtain benefits Congress has made them legally eligible to receive, and such data has [not](#) been historically shared outside of the agency other than to investigate waste, fraud or abuse of the program. While immigrant eligibility for many public benefits is [limited](#), experts [note](#) that immigrant families—including those with U.S.-citizen children who remain eligible for Medicaid—may be chilled from obtaining benefits to which they or their family members are qualified.

AI Adoption Under the Second Trump Administration

Currently, AI-powered technologies such as ImmigrationOS and ELITE function less as autonomous decisionmakers and more as decision-support systems. The software analyzes records and generates a ranked list of leads or an address with a confidence score, while a human agent retains final authority over whether to act on that lead. An ICE official [described](#) this distinction directly, stating that the tools are “not telling us who to arrest, but they are giving us leads and saying, ‘hey, here's all the information about this person.’” From ICE’s perspective, these systems allow agents to [process](#) large quantities of information more quickly, prioritize cases based on agency enforcement objectives, and devote fewer resources to outdated addresses or leads that cannot be verified. In 2026, ICE reported working on [more than 40](#) AI use cases. An agency official also [reported](#) that ELITE produced a successful result approximately 80 percent of the time, compared with 30 percent for ICE’s previous internally developed system. If sustained across operations, more accurate address information could reduce unsuccessful visits, limit encounters with uninvolved residents at outdated addresses, and allow agents to focus on cases that are more likely to result in locating the intended individual.

DHS's [AI Use Case Inventory](#) identifies similar efficiency benefits for facial recognition used in Homeland Security Investigations criminal cases. According to DHS, the technology reduces the time investigators spend manually searching online for images and can identify potentially relevant photographs or profiles that investigators might otherwise miss. DHS maintains that these capabilities can improve the speed and effectiveness of investigations into complex criminal and transnational networks while allowing investigators to devote more attention to corroborating evidence, analyzing relationships, and building cases.

DHS has also reported that HSI's more limited use of facial recognition in child sexual-exploitation investigations has [contributed](#) to identifying victims, rescuing children, and arresting suspected perpetrators, including in previously unresolved cases. In so doing, it emphasizes that these facial-recognition results are investigative leads rather than confirmed identifications. DHS [states](#) that no law-enforcement action may be based solely on a facial-recognition lead; unsuccessful or unverified results are not entered into the investigative record, and trained personnel must document and vet the technology's use under established investigative procedures. This requirement of follow-up verification reflects the government's position that AI can make investigations faster and more comprehensive without transferring final investigative or enforcement authority from trained personnel to an automated system.

Concerns Regarding Expanded Use of Facial Recognition Technologies

Under the second Trump administration, AI-powered facial recognition tools have been increasingly deployed by immigration enforcement to identify removable noncitizens. Legal experts [describe](#) a "drastic shift" from DHS's use of facial recognition technology, which was historically limited largely to investigations and ports of entry and exit. Advocates have [characterized](#) this pattern as "mission creep," arguing that tools originally built and justified for immigration enforcement at the border are steadily being extended far from that original context. During enforcement operations in Minnesota in 2025, ICE reportedly [used](#) two separate facial recognition programs, including Mobile Fortify, to identify people who had been photographed at protests criticizing the agency's operations. Multiple protestors and observers [reported](#) being intimidated by immigration agents using the technologies. In response, civil liberties groups [argued](#) the practice violated the First Amendment, representing monitoring and chilling of constitutionally-protected speech and assembly.

In early 2026, a lawsuit filed by the State of Illinois and the City of Chicago against DHS alleging widespread, "suspicionless" collection of biometric data of bystanders and protestors [disclosed](#) new details confirming how far Mobile Fortify's use had already spread since its June 2025 launch. Court filings [showed](#) the app had been deployed more than 100,000 times nationwide during its first six months of operation, including "extensively during interior enforcement operations in Illinois." The lawsuit also

highlighted DHS's own acknowledgment that the tool could photograph “someone other than an alien, including U.S. citizens or lawful permanent residents,” since the app’s use is not limited to cases of individualized suspicion that someone is out of status or has engaged in criminal conduct and individuals have no ability to opt out of being scanned by a facial recognition technology. Critics, including privacy advocates involved in the litigation, have pointed to the absence of any disclosed retention limit for these images as the central risk. A U.S. citizen who is scanned by this technology and released within minutes can still end up embedded in a federal biometric database for over a decade, available for matching against future encounters, investigations, or other agencies' systems, with no connection to any finding of wrongdoing. Once someone is scanned using these facial recognition tools, there is no public accounting of whether their photo is deleted, stored indefinitely, or shared with other agencies, regardless of whether the initial use of the technology on that person ever led to an arrest.

It was reported in June 2026 that DHS has outlined plans to [extend](#) AI-powered facial recognition capability, as described above, to local law enforcement agencies participating in [the 287\(g\) program](#) through a mobile app called the ICE Task Force Module. With more than 1,300 [departments](#) across 32 states now part of the 287(g) program, widespread implementation of the ICE Task Force Module to these jurisdictions could greatly increase the reach of these tools, scanning thousands of U.S. citizen faces and checking them against massive federal databases, including in non-immigration enforcement contexts. With the effort still in the planning stages, it is [unclear](#) whether the technology would be utilized for routine law enforcement encounters like traffic stops or on a more limited basis. But because the tool was designed specifically to help deputized local law enforcement officers assess whether the removability of people they encounter under immigration law, the implementation of this plan carries a real risk of further [undermining community trust](#) from immigrant communities and others concerned about being swept up by these enforcement efforts.

Governance Gaps in AI-Driven Immigration Enforcement

The technologies outlined above point to several recurring gaps in how such systems are governed. As the U.S. Commission on Civil Rights (USCCR) has [observed](#), federal laws or regulations are limited in how they specifically address the use of facial recognition technology by the federal government. This does not mean existing law is entirely silent on the underlying conduct – several general-purpose statutes may apply in a limited or indirect fashion. The [Privacy Act of 1974](#), for example, establishes controls on how federal agencies collect, maintain, and disclose personal information held in “systems of records,” and USCCR's report notes that the Privacy Act may constrain or limit agency use of facial recognition technology and related data practices. But the law predates modern AI and biometric technology by decades and is not a clear fit for all aspects related to facial recognition or AI-driven immigration enforcement tools.

Additionally, retention periods and access limits for biometric data also remain largely unspecified across the tools examined. The [Privacy Act](#) requires that agencies publish notice of their systems of records and limits disclosure absent an individual's consent or a statutory exception, and separately, the Federal Information Security Modernization Act requires agencies and their contractors to maintain adequate data security programs. Neither statute, however, sets a specific retention period for biometric data, and the USCCR's review [found](#) no federal regulations imposing regular oversight requirements or clear data-handling standards for facial recognition technology. Given this gap, individual departments have taken inconsistent approaches. The Department of Justice's (DOJ) [interim facial recognition policy](#), adopted in December 2023, addresses data retention and requires that facial recognition results serve only as investigative leads rather than a sole basis for arrest, but this policy only applies to DOJ and does not bind DHS, ICE, or CBP.

Individual databases have limited surveillance power on their own but combining them into a single platform with probabilistic targeting creates capabilities far beyond prior database tools. Moreover, those capabilities do not stay confined to ICE's intended targets. ELITE's use of Medicaid and other public-benefits data to generate address confidence scores [draws](#) in household members, family contacts, and anyone else who shares an address or account with an enforcement target, including U.S. citizens and lawful permanent residents who have no connection to the underlying investigation beyond living with or near someone under scrutiny. This spillover is structural, not incidental: ICE's [data-sharing agreement](#) with the Centers for Medicare and Medicaid Services reportedly grants it access to records on nearly 80 million Medicaid enrollees, and health-policy researchers have [noted](#) that immigration status cannot reliably be isolated within that dataset, meaning citizens and lawfully present immigrants are swept into the same enforcement pipeline as undocumented individuals.

The same logic extends beyond ICE itself. Once biometric and household-linkage data are consolidated into a searchable, cross-referenced system, nothing in current law limits which other agencies could access it for purposes having nothing to do with immigration enforcement, raising a number of concerns including undue legal scrutiny on citizens and legal residents. While a conventional, non-AI database-matching tool drawing on the same combination of government records could theoretically generate comparable address and household linkages, the [risks of abuses](#) are heightened by incorporating AI into such a system. What AI adds is the scale and speed at which previously siloed, sensitive records, Medicaid enrollment, DMV files, utility accounts, biometric scans, can now be fused, cross-referenced, and scored automatically, turning a theoretical vulnerability into an operational one.

The result is a set of privacy risks that are genuinely new in degree, if not in kind: citizens, lawful permanent residents, and immigrants alike are now discoverable,

linkable, and trackable through their ordinary interactions with government and commercial systems, entirely independent of their own immigration status or any individualized suspicion of wrongdoing. Absent binding, government-wide limits on retention, access, and downstream use, the risk is that these capabilities will keep expanding faster than the legal framework meant to constrain them. Used responsibly and paired with meaningful oversight, that capability could support more precise, better-targeted enforcement. Deployed without clear limits on data retention, access, and use, however it instead exposes citizens and noncitizens alike to expanded surveillance risk regardless of their own immigration statuses.