What are the legal precedents for ICE using AI-driven migrant tracking?

April 15, 2026 | SnugLab Research | readme.snuglab.com

Executive Summary

There are no definitive judicial rulings that have specifically applied the individualized suspicion requirement from *Carpenter v. United States* to ICE's AI-driven aggregation and analysis of multiple types of third-party data to identify enforcement targets [6, 9, 12]. Instead, ICE's current AI-driven migrant tracking raises significant concerns regarding due process and privacy rights due to insufficient legal oversight and the ongoing legal interpretation of new technologies [4, 11, 14, 18, 25, 26].

Key Findings

Lack of Definitive Legal Precedent for AI-Driven Data Aggregation

Currently, no specific judicial rulings or binding appellate decisions have definitively applied the individualized suspicion requirement from *Carpenter v. United States* to ICE's AI-driven aggregation and analysis of multiple types of third-party data (such as SEVIS, CBP data, commercial databases, and cell phone location data) to identify "enforcement targets" [6, 9, 12]. The research indicates a legal debate regarding whether government purchase of such data constitutes a "search" requiring a warrant under the Fourth Amendment [15]. Some argue that the purchase does not qualify as state action and therefore avoids warrant requirements, while others maintain it should be considered a search [15]. The Supreme Court recognized that a constitutional right to privacy emerges from "penumbras, formed by emanations" of Bill of Rights guarantees, and that the Fourth Amendment protects people, not merely physical spaces, against "every unjustifiable intrusion by the government" [19].

ICE's AI-driven data analysis is argued to constitute a 'search' under the Fourth Amendment requiring individualized suspicion because it aggregates and analyzes extensive personal data to identify individuals, mirroring the long-term tracking deemed unconstitutional in *Carpenter* [13, 5, 6, 8, 12]. A particular concern is ICE's reported

efforts to circumvent the *Carpenter* decision regarding cell-site location information [13].

Transparency, Oversight, and Accountability Challenges

Government oversight does not adequately ensure accountability for errors, abuses, or privacy violations within ICE's AI-driven tracking programs [6, 10, 12]. The reliance on private contractors like Palantir and GEO Group, combined with the proprietary nature of the algorithms used, complicates accountability [10, 12]. ICE's contracts with these companies-potentially totaling $1.2 billion-incentivize speed over accuracy [13]. Palantir has received at least $113 million in federal contracts since 2017 for its data analytics platforms used by ICE [11, 12].

ICE has contracted with thirteen companies for "skip tracing," potentially targeting over one million individuals, with bonuses awarded for quickly verifying locations [13]. This bonus structure demonstrably incentivizes skip-tracing companies to prioritize the speed of location verifications over their accuracy and legal compliance [13]. This reliance on private entities hinders transparency and makes it difficult to assess errors or abuses [17]. The proprietary nature of these algorithms further hinders public oversight [6, 10]. While legislative and administrative actions to increase transparency and oversight are being considered, they face hurdles due to the proprietary nature of algorithms and reliance on private contractors [6, 10, 12].

Algorithmic Bias and Disparate Impact Concerns

The available evidence does not definitively establish a quantifiable magnitude of statistically significant disparity in targeting between racial or ethnic groups resulting from ICE's AI migrant tracking systems that is indicative of systemic bias beyond random variation [4, 5, 11, 20, 21, 22]. However, existing research methods are sufficient to establish the *likelihood* of algorithmic bias in ICE's systems even without complete data access [6, 7, 8]. Experts note that AI can reflect existing racial and gender biases [3].

Legal challenges to government AI systems based on algorithmic bias are increasingly successful in achieving transparency and modifications, though complete invalidation of systems remains rare [16]. Legal theories employed include Equal Protection, alleging discriminatory impact, and Due Process, demanding fair procedures [1, 6, 23]. Evidence presented in these challenges commonly includes statistical disparities demonstrating

unequal outcomes for different groups and expert bias audits [16]. Judicial outcomes have included compelled disclosures of algorithmic information and system modifications to reduce bias [2, 24].

Data Sources and Privacy Risks

ICE utilizes several data sources for AI-driven tracking, including SEVIS, CBP data, commercial databases, and cell phone location data [13]. Among these, cell phone location data presents the greatest risk to individual privacy and due process [13]. This is because it reveals individuals' movements over time, creating detailed patterns of life, and is seen as circumventing the Supreme Court's *Carpenter v. United States* decision, which requires a warrant for extended cell-site location tracking [6, 12, 13]. The agency obtains this data through third-party companies, adding another layer of complexity and potential for abuse [13].

ICE accesses a network of government and private databases, including Thomson Reuters Clear [13]. As one training document detailed, Palantir software allowed ICE agents to search across data from the Student and Exchange Visitor Information System (SEVIS), which "at the time contained 4.9 million records 'of non-immigrant students, exchange visitors and their dependents' dating back to 2016" [13]. The 2025 consolidation of SSA, IRS, and DHS records under Palantir contracts creates a single dataset containing financial records, tax records, immigration status, health records, employment history, and identity data for effectively every American [15].

Ineffectiveness of Legal Remedies

Legal recourse for individuals incorrectly identified or targeted by ICE's AI tracking systems is effectively unavailable due to the high evidentiary burden of proving causation and the opacity of the algorithms [6, 10, 12]. While individuals can pursue legal action related to unlawful search and seizure under the Fourth Amendment, demonstrating a violation is difficult due to the lack of transparency regarding the data sources and algorithms employed by ICE [6, 10, 12]. The proprietary nature of the algorithms hinders public oversight, making it challenging to identify and correct errors [6, 10]. The effectiveness of administrative appeals is questioned, particularly given the scale of surveillance and the lack of independent oversight [10, 12].

Implications

The absence of definitive legal precedents specifically addressing ICE's AI-driven data aggregation means the legal landscape for such technologies is still developing, leaving significant questions about the scope of Fourth Amendment protections in the digital age. The reliance on private contractors and the proprietary nature of AI algorithms create a system with limited public oversight, complicating accountability for errors, abuses, and potential privacy violations. This situation suggests that the increased efficiency provided by AI in location verification may come at the cost of compromising due process and individual privacy. Furthermore, the acknowledged likelihood of algorithmic bias in AI systems, even without specific statistical proof in ICE's context, implies a persistent risk of discriminatory outcomes that existing legal remedies struggle to address effectively due to evidentiary burdens and algorithmic opacity.

Limitations and Caveats

This report draws from a source pool that indicates ongoing legal interpretation of new technology, rather than settled law. A key limitation is the absence of definitive judicial rulings applying *Carpenter v. United States*' individualized suspicion requirement to ICE's AI-driven aggregation of multiple types of third-party data. The available evidence does not definitively establish a quantifiable magnitude of statistically significant disparity in targeting between racial or ethnic groups resulting from ICE's AI migrant tracking systems that is indicative of systemic bias beyond random variation. The proprietary nature of the algorithms used by private contractors also limits public access to complete training data and algorithmic processes, hindering a full assessment of bias and errors. Additionally, the research does not detail specific legislative or administrative actions currently being considered to increase transparency and oversight, nor does it provide detailed cost breakdowns for specific commercial databases utilized by ICE.

Sources

[1] [edu] Viewcontent.Cgi - repository.law.umich.edu - https://repository.law.umich.edu/cgi/viewcontent.cgi?article=3061&context=articles
[2] [edu] Viewcontent.Cgi - scholarship.law.umn.edu - https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1590&context=mjlst
[3] [edu] Viewcontent.Cgi - scholarship.law.uc.edu - https://scholarship.law.uc.edu/cgi/viewcontent.cgi?article=1045&context=ipclj

[4] [gov] Ice - dhs.gov - https://www.dhs.gov/ai/use-case-inventory/ice

[5] [edu] Accountability In Immigration Dhs Faces Pushback Over Rapid - lawreview.syr.edu - https://lawreview.syr.edu/accountability-in-immigration-dhs-faces-pushback-over-rapid-a-i-expansion/

[6] [edu] Viewcontent.Cgi - scholarship.richmond.edu - https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1491&context=jolt

[7] Dhs Is Circumventing Constitution By Buying Data It Would No - aclu.org - https://www.aclu.org/news/privacy-technology/dhs-is-circumventing-constitution-by-buying-data-it-would-normally-need-a-warrant-to-access

[8] [edu] Data Justice Act - law.nyu.edu - https://www.law.nyu.edu/documents/data-justice-act

[9] [gov] Dl - justice.gov - https://www.justice.gov/jmd/media/1434716/dl?inline

[10] [edu] Striking A Balance - avemarialaw.edu - https://www.avemarialaw.edu/striking-a-balance/

[11] [blog] Ice Bounty Hunters Use Ai Track Immigrants - americanimmigrationcouncil.org - https://www.americanimmigrationcouncil.org/blog/ice-bounty-hunters-use-ai-track-immigrants/

[12] [edu] Viewcontent.Cgi - repository.law.indiana.edu - https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1057&context=ipt

[13] [news] Ice Palantir Data - theguardian.com - https://www.theguardian.com/us-news/ng-interactive/2025/sep/22/ice-palantir-data

[14] [news] Ice Surveillance Data Brokers Congress Anthropic - npr.org - https://www.npr.org/2026/03/25/nx-s1-5752369/ice-surveillance-data-brokers-congress-anthropic

[15] Palantir Gotham - sbytec.com - https://www.sbytec.com/vulnerabilities/palantir-gotham/

[16] [gov] acis.eoir.justice.gov - https://acis.eoir.justice.gov/

[17] [edu] Viewcontent.Cgi - scholarship.law.uc.edu - https://scholarship.law.uc.edu/cgi/viewcontent.cgi?article=1391&context=uclr

[18] [gov] Cbp - dhs.gov - https://www.dhs.gov/ai/use-case-inventory/cbp

[19] [edu] Put The Katz Back In The Bag Restoring Privacy Rights In The - sjipl.mainelaw.maine.edu - https://sjipl.mainelaw.maine.edu/2025/10/27/put-the-katz-back-in-the-bag-restoring-privacy-rights-in-the-digital-age/

[20] [edu] AI has a bias problem. Can we build something smarter? - https://news.berkeley.edu/2026/01/20/ai-has-a-bias-problem-can-we-build-something-smarter/

[21] [edu] Artificial intelligence and algorithmic exclusion - Brookings Institution - https://www.brookings.edu/articles/artificial-intelligence-and-algorithmic-exclusion/

[22] AI Trends For 2026 - AI and Algorithmic Bias in Financial Services - https://www.mofo.com/resources/insights/260127-ai-trends-for-2026-ai-and-algorithmic-bias

[23] RANDOMIZING IMMIGRATION ENFORCEMENT - NYU Law Review - https://www.nyulawreview.org/wp-content/uploads/2018/08/NYULawReview-88-5-Benin.pdf

[24] [edu] Deportation and Immigration Enforcement in the United States - PINES - https://pines.bemidjistate.edu/cgi/viewcontent.cgi?article=1138&context=capstone-polisci

[25] [edu] Big Data and Automated Decision-Making Systems in Immigration Law - https://www.law.georgetown.edu/immigration-law-journal/wp-content/uploads/sites/19/2020/08/Weapons-of-Mass-Deportation-Big-Data-and-Automated-Decision-Making-Systems-in-Immigration-Law.pdf

[26] how U.S. immigration enforcement uses data and AI to ... - GitHub Gist - https://gist.github.com/ruvnet/da9609939270e3870de465a63352b005