

RATIO CONSULTORES

LEGAL ANALYSIS MEMORANDUM — INTERNAL USE

Palantir Technologies' operational framework for ICE and state police departments, in light of the judicial oversight standard set in Chatrie v. United States, 609 U.S. ____ (2026)

I. PURPOSE OF THE MEMORANDUM

The purpose of this memorandum is to analyze the legal and contractual framework governing the activity of Palantir Technologies Inc. ("Palantir") in its role as a provider of data infrastructure and analytics to the U.S. Department of Homeland Security —through its component Immigration and Customs Enforcement ("ICE")— and to various state and local police departments, in order to determine to what extent that framework satisfies the judicial oversight requirements established by the majority opinion of the U.S. Supreme Court in *Chatrie v. United States*, No. 25-112, decided on June 29, 2026.

The analysis is structured in four parts: (i) a factual and contractual reconstruction of Palantir's role vis-à-vis ICE and state police forces; (ii) a summary of the judicial oversight standard set by the majority in *Chatrie*; (iii) a point-by-point comparison between the two; and (iv) a reference to the related regulatory framework and the status of ongoing litigation on the matter.

II. FACTUAL AND CONTRACTUAL FRAMEWORK OF PALANTIR

A. Contractual relationship with ICE

Since 2014, Palantir has operated ICE's Investigative Case Management ("ICM") system, under successive sole-source awards, without a competitive process. An agency contract document describes ICM as "based on Palantir's proprietary solution, already configured specifically for ICE's operational needs." In April 2025, ICE awarded Palantir an additional \$30 million contract to develop ImmigrationOS, a platform designed to: (i) speed up the identification and apprehension of individuals prioritized for removal; (ii) track and report self-deportations with near real-time visibility; and (iii) optimize the logistics of the deportation process. Running on that same infrastructure is the ELITE tool (Enhanced Leads Identification & Targeting for Enforcement), which receives addresses of individuals from the Department of Health

and Human Services (including Medicaid records) and other sources, generating for each individual a dossier and a "confidence score" regarding their current address.

According to reports from organizations specializing in civil liberties (ACLU, Electronic Frontier Foundation) and investigative media outlets (404 Media, Wired, Politico), the data feeding these platforms comes from highly heterogeneous sources: passport records, Social Security information, IRS tax data, automatic license plate readers, flight data, driver's license scans, and cell phone records.

B. Contractual relationship with state and local police forces

Through its Gotham platform, Palantir provides police departments—including the NYPD, LAPD, and the New Orleans Police Department—with a data integration and correlation tool that allows searching for individuals by name, physical characteristics (tattoos, scars), organizational affiliation, or family and social ties, based on the merging of incident reports, arrests, citations, license plate reader data, field interviews, arrest warrants, booking photographs, and state law-enforcement telecommunications databases.

A critical aspect reported by investigative bodies is that much of this information exchange occurs through "fusion centers"—regional hubs administered with the participation of the Department of Homeland Security—and that, unlike other means of obtaining evidence, police agencies would not need, within that circuit, a prior court order to access the data available there.

C. The strategy of acquiring data through commercial or interagency channels (the "data broker loophole")

The most relevant aspect for purposes of this memorandum is the existence of a legal theory maintained by ICE itself, according to which the agency could query commercial location data without a court order, to the extent that such data comes from third-party providers (data brokers) rather than directly from telecommunications companies. Privacy advocacy organizations have characterized this practice as a direct circumvention of the standard set in *Carpenter v. United States* (585 U.S. 296 (2018)), a precedent that—as detailed in the following section—constitutes the direct doctrinal basis for Chatrle.

On the legislative front, a group of thirty federal lawmakers (led by Representatives Goldman and Velázquez and Senator Wyden) sent a formal request for information to ICE and the Department of Homeland Security in April 2026, requiring that all databases and applications used to support immigration enforcement operations be identified, that it be specified which were developed by Palantir or other private contractors, and that the legal authority invoked for the collection and retention of information on U.S. citizens be clarified.

III. THE JUDICIAL OVERSIGHT STANDARD SET IN CHATRIE V. UNITED STATES

As previously developed in our earlier memorandum on this ruling, the Supreme Court majority (opinion by Justice Kagan, joined by Chief Justice Roberts and Justices Sotomayor, Kavanaugh, and Jackson) held that government access to a cell phone's location information—even for a brief period and even when the data was provided by a third-party technology company—constitutes a "search" under the Fourth Amendment, insofar as the individual retains a reasonable expectation of privacy over that information.

From the Chatrie doctrine—integrated with the Carpenter precedent, which it reaffirms and extends—five requirements of judicial oversight directly relevant to this analysis can be drawn:

- Involvement of a neutral and disinterested magistrate: the reasonableness of a search requires, save for exigency exceptions, that a magistrate—not the acting officer—authorize access to the information.
- Individualized probable cause: the magistrate must find a reasonable probability that the information sought exists in the indicated location and will be useful for the investigation of a specific crime.
- Particularity at each stage of the search process: when the procedure is structured in successive stages narrowing a broad universe of people down to an identified subset (as occurred with the three-step geofence warrant in Chatrie), each stage must be described with sufficient particularity, and the selection criteria for advancing from one stage to the next cannot be left to the officer's

unguided discretion, absent any standard set by the magistrate, as specifically developed in Justice Jackson's concurrence.

- Rejection of the third-party doctrine for qualitatively revealing information: the Court reaffirmed that information such as location history, emails, photographs, or medical records is not considered "truly shared" with the third party that stores it, in the sense required by the Miller and Smith doctrine, precisely because it is indispensable to modern life and the user continues to regard it as their own.
- Rejection of any "grace period" based on brevity or indirect acquisition: neither the short duration of the period examined nor the fact that the data came from a third party exempts the State from the warrant requirement; the Court was explicit that these circumstances do not lessen the constitutional concern over "too permeating police surveillance."

IV. COMPARATIVE ANALYSIS

The following table compares each of the standards outlined above with Palantir's reported operational model in its role as an infrastructure provider for ICE and for state police departments.

Requirement set by the Chatree majority	Palantir / ICE / state police operational model	Is it satisfied?
Involvement of a neutral, disinterested magistrate before access to sensitive information.	A large part of the data flow feeding Gotham, ImmigrationOS, and ELITE comes from interagency fusion centers and from purchases from data brokers, channels in which —according to specialized reports— no court order is required at all.	NO
Individualized probable cause as to each person whose data is obtained.	Tools such as ELITE generate dossiers and "confidence scores" regarding a person's address based on massive databases (Medicaid/HHS and other sources) without any reported standard of prior probable cause per individual.	NO
Particularity at each stage of the process, with criteria set by the magistrate (not by the officer) for	The narrowing of the universe of subjects in Gotham/ELITE is carried out by the analyst or by the platform's own algorithm, without	NO

"narrowing" the universe of persons subject to greater scrutiny.	judicial involvement setting the selection criteria in advance.	
Rejection of the third-party doctrine when the information is qualitatively "revealing" (emails, photos, calendars, location history).	The data comprising these platforms (medical history, Medicaid records, license plates, location) is of the same type as, or more sensitive than, that protected in <i>Chatrle</i> ; it is acquired through channels (commercial purchase, interagency agreements) that seek precisely to circumvent that doctrine.	NO
Rejection of a "grace period" based on short duration or third-party origin.	ICE's reported institutional justification maintains the opposite premise: that data obtained through commercial brokers, rather than directly from the original provider, would fall outside the perimeter of the Fourth Amendment.	NO

The foregoing comparison shows that the point of friction does not, strictly speaking, lie in Palantir's software considered in the abstract, but rather in the manner in which the data loaded into it is obtained. Palantir presents itself—and largely acts—as a layer of aggregation, correlation, and visualization of information that the agencies already possess or acquire through other means; the defect in judicial oversight is located primarily at that prior acquisition stage (purchase from data brokers, interagency agreements, fusion centers), before the information enters the platform.

Notwithstanding the foregoing, the product's architecture is not neutral with respect to the problem: by enabling a progressive "narrowing" process from broad universes of people down to individualized target lists—in a manner structurally analogous to the three-stage geofence warrant process examined in *Chatrle*—without a magistrate defining in advance the selection criteria at each stage, the software reproduces precisely the defect that Justice Jackson identified as insufficient to satisfy the particularity requirement.

V. RELATED REGULATORY FRAMEWORK AND STATUS OF LITIGATION

On the legislative front, the bill known as the Fourth Amendment Is Not For Sale Act (H.R. 4639, 118th Congress, with successive reintroduced versions) seeks precisely to close the so-called "data broker loophole," requiring a court order for the

government to access sensitive information—including location data— regardless of whether it is obtained directly from the original provider or from a commercial data broker. As of the date of this memorandum, that bill has not been enacted as federal law.

On the judicial front, there are precedents of active litigation addressing related issues, although none has yet specifically resolved the application of the Chatrie doctrine to Palantir's platforms:

- *State of Illinois and City of Chicago v. ICE* (January 2026): a lawsuit over the use of the Mobile Fortify facial recognition application on more than 100,000 occasions, challenging its compatibility with state privacy laws and with the scope of the agency's statutory authority.
- *Nguyen v. State (Texas)*: pending litigation on the constitutionality of geofence warrants, specifically challenging that such procedures authorize indiscriminate searches without probable cause as to all persons included, and that they allow officers to decide, without judicial oversight, which users to subject to greater scrutiny in subsequent stages — a particularity objection structurally identical to the one developed in this memorandum.
- *Warrantless home entry cases in Minnesota* (January 2026): a federal district judge ordered the release of a detainee after finding that ICE agents entered his home without presenting a valid warrant, as part of the so-called "Operation Metro Surge," an operation in which the use of facial recognition tools and the ELITE application was reported.

It should be noted that Palantir has publicly rejected criticism directed at its role, maintaining that all of its government contracts are exclusive to each contracting agency, with specific legal, procedural, and technical safeguards, that information sharing between agencies is governed by data-sharing agreements subject to oversight, and that its platforms maintain an indelible audit trail of all interactions. Its CEO, Alex Karp, has publicly argued that the company's product, by design, requires compliance with Fourth Amendment protections. These claims, however, have not been judicially validated to date, and refer primarily to internal traceability controls rather than to the existence of ex ante judicial oversight over data acquisition.

Brief reference should also be made to the computing infrastructure agreement entered into between Palantir and NVIDIA Corporation —initially announced in October 2025 and expanded on June 29, 2026— under which both companies integrate NVIDIA's Blackwell Ultra graphics processing units and Nemotron open models with Palantir's Ontology, Foundry, AIP, and Apollo platforms, under the name "Sovereign AI Operating System," intended for U.S. government agencies and critical infrastructure operators requiring deployment in isolated environments (on-premise or air-gapped).

This agreement, in itself, does not violate the standard set in *Chatrie v. United States*: it is a computing infrastructure agreement —the provision of hardware and artificial intelligence models— and not a mechanism for the State's acquisition of location or behavioral data, which is precisely the object of judicial oversight that *Chatrie* requires. As of the date of this memorandum, there is no public record that ICE has specifically adopted this infrastructure to operate Gotham, ELITE, or ImmigrationOS.

The following caveat should nonetheless be noted: to the extent that this infrastructure comes to be deployed to accelerate the operation of those platforms, its practical effect would not be to create a new form of constitutional violation, but rather to aggravate the defect already identified in Section IV of this memorandum —namely, the greater speed and algorithmic autonomy in the process of "narrowing" broad universes of people down to individualized target lists, without a magistrate setting the selection criteria at each stage in advance, in accordance with the particularity objection developed by Justice Jackson in her concurrence. This is, in any event, a hypothesis of future application and not a verified fact as of the date of this memorandum, and it is suggested that it be monitored.

VI. CONCLUSIONS

1. The framework described for ICE and for the state police departments that use Palantir's Gotham, ImmigrationOS, and ELITE platforms does not satisfy, in its currently reported form, the judicial oversight requirements established by the majority opinion in *Chatrie v. United States*, particularly with respect to: (i) the absence of involvement by a neutral magistrate in much of the data-acquisition circuit; (ii) the lack of any reported standard of individualized probable cause; (iii) the judicially uncontrolled delegation of the process of "narrowing" broad universes of people down

to target lists; and (iv) the persistence of a data-acquisition strategy through commercial or interagency channels that seeks precisely to circumvent the third-party doctrine that Chatrle —following Carpenter— refused to apply to qualitatively revealing information.

2. This conclusion constitutes a comparative analysis of doctrinal compatibility, not a judicial determination: as of the date of this memorandum, no U.S. court has issued a ruling specifically applying the Chatrle standard to the Palantir platforms used by ICE or by state police forces. The ongoing litigation over geofence warrants (*Nguyen v. State*) and over other related surveillance practices (*Illinois/Chicago v. ICE*; *Minnesota cases*) could, in the coming months, produce directly applicable precedent.

3. It is suggested that the evolution of the Fourth Amendment Is Not For Sale Act at the federal level be monitored, as well as the rulings issued in the individual cases referenced in Section V, insofar as they constitute the most likely ground for the concrete judicial application of the Chatrle standards to this type of data architecture.

VII. SOURCES CONSULTED

Chatrle v. United States, 609 U.S. ____ (2026) (slip op.). — *Carpenter v. United States*, 585 U.S. 296 (2018). — American Civil Liberties Union, "All the Ways Palantir is Assisting Trump's Abusive Removal Campaign" (April 2026). — Electronic Frontier Foundation, "Report: ICE Using Palantir Tool That Feeds On Medicaid Data" (January 2026) and "Palantir Has a Human Rights Policy. Its ICE Work Tells a Different Story" (April 2026). — Palantir Technologies, "Correcting the Record: Response to the EFF January 15, 2026 Report on Palantir" (corporate blog, January 2026). — Vanderbilt Law School, "Eyes Everywhere: ICE's Expanded Use of Surveillance Technologies" (February 2026). — Office of Representative Daniel Goldman, joint statement with Representative Nydia Velázquez and Senator Ron Wyden (April 2026). — American Immigration Council, "ICE to Use ImmigrationOS by Palantir" (2025). — Campaign Zero, "The Private Companies Quietly Building a Police State" (October 2025). — AFSC Investigate, corporate profile "Palantir Technologies Inc." — The Register, "Palantir declares itself the guardian of Americans' rights" (February 2026). — NPR, "ICE has spun a massive surveillance web" (March 2026). — Biometric Update, "ICE advances sole source deal with Palantir for new surveillance backbone" (2025-2026). — Fourth Amendment Is Not For Sale Act, H.R. 4639, 118th Congress. — Palantir Technologies / NVIDIA Corporation, joint announcement "Sovereign AI Operating System" (October 2025 and June 29, 2026).

Methodological note: this memorandum was prepared on the basis of specialized news sources, reports from civil-rights organizations, statements from the company itself, and publicly available contractual documents as of the date indicated. It does not substitute for direct review of the specific

contracts and data-sharing agreements, access to which might require FOIA requests or discovery in the context of specific litigation.