Forensic Audit of Transnational Cyber-Surveillance Ingestion and Warrantless Municipal Geolocation Tracking (FY 2025–2026)

Procurement Channels and State-Level Grants

The acquisition of proprietary, foreign-developed cyber-surveillance platforms by local municipal purchasing hubs is characterized by a reliance on non-competitive procurement vehicles and federal grant funding streams. To bypass localized competitive bidding laws, civil rights reviews, and public city council hearings, local law enforcement and prosecutorial bodies routinely route purchases through third-party "Master Aggregators". Carahsoft Technology Corporation serves as the primary distributor and master aggregator for Voyager Labs and associated digital tracking systems. This distributor structure allows municipal agencies to rapidly acquire proprietary software licenses through pre-negotiated information technology schedules, including the General Services Administration Multiple Award Schedules, California Multiple Award Schedules, and National Association of State Procurement Officials ValuePoint cooperative contracts.

Forensic analysis of municipal contract records from FY 2024 through May 2026 reveals a consistent pattern of sole-source justification models and subscription renewals designed to evade public oversight. The Queens County District Attorney's office, under procurement PIN# QDA20230406, executed a sole-source subscription renewal for Cobwebs Technologies' integrated Tangles and WebLoc platforms for a contract term spanning June 2, 2023, to June 1, 2024, certifying Cobwebs as the only authorized source for Web Intelligence Investigation software under one unified interface. This municipal purchasing pipeline extended into the Bronx County District Attorney's office, which initiated a sole-source intent to award under PIN# 902S24001 for Cobwebs' integrated web intelligence platform, designating the system as exempt from standard competitive bids due to Cobwebs' retention of all proprietary source code and refusal to issue licenses to other resellers.

These localized procurement channels are heavily financed by federal non-disaster grant funding outlays administered by the Department of Homeland Security. Specifically, high-density metropolitan areas and regional fusion centers utilize the Urban Area Security Initiative to cover the recurring annual subscription costs of systems like Cobwebs' Tangles and Voyager Analytics under the administrative classification of "preventing domestic terrorism". Additionally, the Homeland Security Grant Program provides broader federal-to-local funding conduits that bypass local general fund budget audits, shielding high-capital acquisitions from municipal taxpayer scrutiny.

—►—►

This grant-reliance model is reflected in the pricing proposals exchanged during the transition from pilot trials to multi-year contracts. The Los Angeles Police Department, which initiated a four-month evaluation trial of Voyager Labs' platform in 2019 using discretionary investigative

funding , subsequently negotiated a three-year direct acquisition contract. Pricing proposals from Voyager Labs outlined a baseline annual license fee of $705,000 for VoyagerAnalytics—which was discounted to $394,800 under a multi-year commitment—alongside a $54,750 base fee for the Profile Finder module (discounted to $30,660) and $50,000 for twenty-five dedicated user licenses (discounted to $28,000). Meanwhile, the New York City Police Department established a multi-million-dollar relationship with Voyager Labs, executing a $9 million contract for Voyager Analytics and Genesis software platforms in 2018, followed by a $1.6 million service renewal in 2021. The NYPD subsequently expanded its vendor portfolio to include Cobwebs Technologies' Tangles and WebLoc products under an annual contract published in the city record.

Data Telemetry Handshakes and API Routing Architecture

The technical functionality of these surveillance platforms is rooted in automated data-routing protocols and application programming interface handshakes designed to extract both open-source and private user metadata. Cobwebs Technologies' WebLoc module functions as an ad-based geolocation surveillance system that is sold as an add-on product to the Tangles web intelligence platform. The WebLoc system obtains mobile device telemetry directly from Software Development Kits embedded in commercial mobile applications and Real-Time Bidding digital advertising data streams. WebLoc's API architecture ingests a continuously updated stream of records from up to 500 million mobile devices globally. This telemetry includes unique mobile device identifiers (advertising IDs), precise latitude and longitude coordinate coordinates, and demographic profile data harvested from ad networks.
—► —► —►

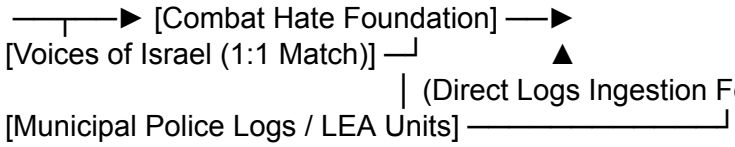
Within the Tangles software interface, this location telemetry is matched with standard features engineered to extract metadata from deleted or suspended accounts, run graph and cross-analyses of target subjects, and deploy automated geolocation geofences. Municipal operators utilize WebLoc to monitor and map the movements of entire populations up to three years in the past. By implementing virtual geofenced boundaries around specific political protest assemblies, local fusion centers generate automated, real-time alerts when targeted devices enter a preselected range. This spatial intelligence bypasses the judicial requirement to present probable cause to a judge to obtain a warrant for cell phone location records, a practice that directly circumvents the constitutional protections established under *Carpenter v. United States*. Concurrently, Voyager Labs uses proprietary algorithms and scraping frameworks to construct social network profiles and map associations. To extract data from privacy-restricted platforms, Voyager's software deployed more than 38,000 fake user accounts to bypass Meta's platform security, systematically scraping viewable profile information, posts, likes, comments, friend lists, photos, and group memberships from more than 600,000 Facebook and Instagram users. Once this data is ingested, Voyager compiles automated Friendship Reports. The Friendship Report API generates an exportable, deep-dive map of the connections between users, documenting mutual friendships, the exact date the connection was established, and the frequency of interaction between the target and their associations. Voyager's risk engine applies machine learning models to unstructured text and visual media to evaluate subjective criteria, such as a target's "passion" levels, and generates a color-coded risk score predicting their "affinity for fundamentalism or extremism". These risk scores are routed directly into municipal

Real-Time Crime Centers to drive preemptive policing, introducing severe algorithmic bias by targeting cultural heritage, religious text references, and linguistic markers.

The Closed-Loop Public-Private Surveillance Interface

The localized data telemetry and network maps generated by municipal surveillance software are structurally funneled into a synchronized, private threat intelligence framework managed by the Combat Antisemitism Movement and its Antisemitism Research Center. Legally controlled and shielded by the Combat Hate Foundation—a Moundridge, Kansas-registered public charity governed by corporate officers of Berexco LLC—the Combat Antisemitism Movement is financed through multi-million-dollar philanthropic injections from the Robert M. Beren Foundation. This financial foundation is augmented by a 1:1 sovereign state-matching framework with Voices of Israel Ltd., a public-benefit company operating under the direction of the Israeli Ministry of Diaspora Affairs.

The alignment between CAM's advocacy and state security structures is maintained through leadership crossovers, including board member Sima Vaknin-Gil, the former Chief Censor of the Israel Defense Forces and former Director-General of the Ministry of Strategic Affairs. To manage its domestic policy-steering and database integration without triggering registration under the Foreign Agents Registration Act, CAM employs domestic lobbying firms under the domestic Lobbying Disclosure Act database, utilizing transparency gaps to obscure foreign state-aligned funding sources.



The operational interface between local police departments and CAM's private database relies on the Municipal Antisemitism Action Index, a policy blueprint administered by CAM's Mayors Advisory Board. Under this framework, municipal law enforcement agencies undergo training modules that anchor local policing codes and safety protocols to the International Holocaust Remembrance Alliance working definition of antisemitism. This localized administrative rulemaking instructs police officers to reclassify non-violent political expression, protest slogans, and anti-Zionist public graffiti as bias incidents or potential hate crimes.

Once these localized incidents are reclassified in municipal police logs, they are programmatically routed from local police databases directly into CAM's centralized ARC repository. This data integration loop creates a closed-loop threat intelligence feed targeting domestic political protest assembly. This ingestion pipeline operates through specific geographic nodes:

- **The Los Angeles Metro Corridor:** Managed by Beverly Hills Mayor Sharona Nazarian and Riverside Mayor Patricia Lock Dawson, this corridor focuses on integrating local law enforcement reporting with the centralized ARC database and formulating regional police reporting templates linked to the ARC platform.
- **The Atlanta Metro Suburbs:** Led by Sandy Springs Mayor Rusty Paul and Union City Mayor Vince Williams, this node hosted regional collaborative forums to align suburban policing databases and local public safety resolutions with CAM's database tracking systems.

This public-private ingestion loop is mirrored in the academic and technical incubator sector.

The Adir Challenge Foundation acts as a technical incubator, collaborating with Google Jigsaw's Perspective API to refine natural language processing models against large datasets. It has engineered crowdsourced platforms such as Reportify (designed by Danielle Sobkin and Hannah Levin) and Oct7 Community OS (designed by Omer Dagan and Alan Feld). These platforms automate college campus incident reporting and coordinate digital mobilization campaigns. They function as civilian-facing pipelines that feed qualitative reports and user data back into core NLP models and private databases, paralleling the structural data-routing protocols utilized by municipal police forces to funnel local telemetry into the centralized ARC repository.

Forensic Procurement Ledger Matrix

Purchasing Local Agency	Associated Private Vendor	Deployed Software Platform/Module	Disclosed Contract Transaction Value	Target Data Destination Hub
Queens County District Attorney's Office	Cobwebs Technologies (PenLink, Ltd.)	Tangles & WebLoc Integration Platform	Undisclosed (Sole-source PIN# QDA20230406; June 2, 2023 – June 1, 2024)	CAM Antisemitism Research Center (ARC) Centralized Database / Municipal Ingestion Loop
Bronx County District Attorney's Office	Cobwebs Technologies (PenLink, Ltd.)	Tangles & WebLoc Integration Platform	Undisclosed (Sole-source PIN# 902S24001; September 2023)	CAM Antisemitism Research Center (ARC) Centralized Database / Municipal Ingestion Loop
New York City Police Department (NYPD)	Voyager Labs Ltd. / Cobwebs Technologies	Voyager Analytics & Genesis / Tangles & WebLoc	$9,000,000 (2018 Contract) / $1,600,000 (2021 Renewal) for Voyager; Undisclosed for Cobwebs	NYPD Real-Time Crime Center (RTCC) / CAM Antisemitism Research Center (ARC) Centralized Database
Los Angeles Police Department (LAPD) Tech Units	Voyager Labs Ltd.	Voyager Platform (VoyagerAnalytics, Genesis, Friendship Report)	Undisclosed (4-Month Trial in 2019; Proposed 3-Yr Contract Base Price $809,750 / Discounted to $453,460 annually)	CAM Antisemitism Research Center (ARC) Database / Regional Police Reporting Templates
Washington, D.C. Homeland Security & Emergency Management Agency (HSEMA)	Cobwebs Technologies (PenLink, Ltd.)	Tangles (Web Intelligence Platform)	$348,613.70 (4-Year Licensing, 2020–2024)	District Fusion Center Repository / Downstream Federal-Local Repositories

Purchasing Local Agency	Associated Private Vendor	Deployed Software Platform/Module	Disclosed Contract Transaction Value	Target Data Destination Hub
Panama City Beach Police Department (PCBPD)	Cobwebs Technologies (PenLink, Ltd.)	Tangles / Investigative Software Package	$50,810.00 (3-Year Term, August 2023 – August 2026)	PCBPD Internal Logs / Regional Florida Fusion Centers
Suburban Atlanta Regional Procurement Desks (Sandy Springs / Union City)	Cobwebs Technologies / Associated Vendors	Suburban Surveillance / Local Police Logs	Undisclosed (January 2026 Database Ingestion Forums)	CAM Antisemitism Research Center (ARC) Centralized Database / Regional Collaborative Sub-Hub
U.S. Immigration and Customs Enforcement (ICE)	PenLink, Ltd. (Cobwebs Technologies)	WebLoc (Location Tracking Module)	Undisclosed (2025 No-Bid Contract)	ICE Advanced Immigrant Tracking Systems / DHS Central Repositories

Analysis of Technical and Jurisdictional Overlap

The structural overlap between local police data collection and private threat intelligence databases establishes a parallel tracking mechanism that operates outside the boundaries of standard judicial review. By utilizing WebLoc's ad-based geofencing capabilities, municipal agencies compile location telemetry from commercial streams that map device movements across domestic jurisdictions. The subsequent reclassification of these movements under local municipal safety codes—anchored to specialized definitions of discrimination—allows police units to log political protest activity as civil rights infractions.

Because these reclassified records are routed directly into CAM's private, centralized ARC database, they are insulated from state-level open records laws (such as the Texas Public Information Act or the New York Freedom of Information Law), which only govern public, government-held records. This architecture enables a closed-loop system where public police power is used to collect intelligence that is immediately transferred to private entities. These private entities then use the compiled metrics to lobby for enhanced federal law enforcement interventions, creating an ongoing feedback loop of warrantless surveillance and political monitoring.

Works cited

1. Cobwebs Technologies Web Intelligence Investigation Platform RENEWAL SUBSCRIPTION - The City Record Online (CROL) | Notice Details, https://a856-cityrecord.nyc.gov/RequestDetail/20230406118 2. The City Record Online (CROL) | Notice Details - NYC.gov, https://mspwvw-dcscpfvp.nyc.gov/RequestDetail/20230828102 3. VoyagerAnalyticsTM - Brennan Center for Justice, https://www.brennancenter.org/sites/default/files/2021-11/J0-%20Pricing%20Proposals%20June%202020-June%202021.pdf 4. Exclusive: LAPD partnered with tech firm that enables secretive online spying | US policing | The Guardian, https://www.theguardian.com/us-news/2021/nov/17/los-angeles-police-surveillance-social-media

-voyager 5. NYPD spent millions to contract with firm banned by Meta for fake profiles - The Guardian, https://www.theguardian.com/us-news/2023/sep/08/new-york-police-tracking-voyager-labs-meta-contract 6. NYPD Has Spent Millions of Dollars on Social Media Analysis Tools | Criminal Legal News, https://www.criminallegalnews.org/news/2024/feb/15/nypd-has-spent-millions-dollars-social-media-analysis-tools/ 7. Open Source Collection Operations Tool Interface Requirements - Unicorn Riot, https://unicornriot.ninja/wp-content/uploads/2024/06/cobwebs_and_tangles_redacted.pdf 8. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 KALPANA SRINIVASAN (237460) ksrinivasan@susmangodfrey - Courthouse News, https://www.courthousenews.com/wp-content/uploads/2024/05/meta-platforms-v-voyager-labs-complaint.pdf 9. Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech, https://citizenlab.ca/research/analysis-of-penlinks-ad-based-geolocation-surveillance-tech/ 10. Texas Officers Invested Millions in a Shadowy Phone-Tracking Software. They Won't Say How They've Used It. | Pulitzer Center, https://pulitzercenter.org/stories/texas-officers-invested-millions-shadowy-phone-tracking-software-they-wont-say-how-theyve 11. Meta Sues Surveillance Firm That Worked with Police | Brennan Center for Justice, https://www.brennancenter.org/our-work/analysis-opinion/meta-sues-surveillance-firm-worked-police 12. News Digest: ICLMG remembers Quebec city mosque victims & renews commitment to fight Islamophobia; Letter & action: Following federal court order, bring all Canadians detained in NE Syria home & more - Constant Contact, https://myemail.constantcontact.com/News-Digest--ICLMG-remembers-Quebec-city-mosque-victims---renews-commitment-to-fight-Islamophobia--Letter---action--Following-fe.html?soid=1110839102458&aid=__uYjsNhZGM 13. Documents Reveal How DC Police Surveil Social Media Profiles and Protest Activity, https://www.brennancenter.org/our-work/analysis-opinion/documents-reveal-how-dc-police-surveil-social-media-profiles-and-protest 14. S.T.O.P.: Putting a Check on Unchecked Local N.Y. Government Surveillance | Electronic Frontier Foundation, https://www.eff.org/deeplinks/2023/11/stop-putting-check-unchecked-local-ny-government-surveillance