The Architecture of Municipal Surveillance: Exposing the Cyber-Intelligence Pipelines, Federal Grant Mechanisms, and Data Syndication Networks in the Combat Antisemitism Movement

Executive Overview

The contemporary landscape of municipal law enforcement in the United States is undergoing a profound and highly orchestrated technological transformation. Characterized by the rapid integration of advanced open-source intelligence (OSINT), sophisticated social media scraping algorithms, and location-tracking digital platforms, capabilities historically reserved for federal intelligence agencies and international counter-terrorism task forces are systematically cascading down to local police departments. A critical, exhaustive examination of commercial procurement pipelines reveals a complex, multi-nodal network through which foreign-state-affiliated cyber-intelligence firms—most notably the Israeli-founded entities Cobwebs Technologies and Voyager Labs—have penetrated U.S. municipal infrastructure.

This penetration is not occurring organically or in a political vacuum. The empirical evidence indicates a coordinated policy deployment facilitated by well-funded advocacy networks, prominently the Combat Antisemitism Movement (CAM) and its recently established Mayors Advisory Board. Through highly targeted municipal engagement, these organizations advocate for standardized policy frameworks, such as the Municipal Antisemitism Action Index. These policy frameworks inherently mandate the enhancement of digital monitoring, the adoption of specific, expansive definitions of hate crimes, and the syndication of local threat data to centralized, privately managed databases like CAM's Antisemitism Research Center (ARC).

To bypass local budgetary constraints, municipal oversight committees, and civil liberties watchdogs, the acquisition of these advanced surveillance platforms is heavily subsidized through opaque federal conduits. The primary financial instruments enabling this architecture are the Urban Area Security Initiative (UASI) and the Homeland Security Grant Program (HSGP). By branding predictive policing, algorithmic social graph mapping, and warrantless tracking as critical counter-terrorism and public safety infrastructure, municipal governments and regional fusion centers routinely authorize sole-source procurements or leverage massive cooperative purchasing vehicles. These mechanisms obscure the acquisition of software capable of conducting predictive profiling and deep-dive association mapping—such as Voyager Labs' controversial "Friendship Report"—from the public record.

This comprehensive research report provides a granular, exhaustive analysis of the interconnected nodes comprising this ecosystem. It unpacks the political vanguard driving municipal adoption, dissects the technical capabilities and legal controversies surrounding the surveillance platforms, maps the federal financial instruments utilized to circumvent local budget

scrutiny, and exposes the digital pathways that ultimately funnel localized police tracking data into private, ideologically driven intelligence repositories.

The Post-9/11 Paradigm and the Evolution of Municipal Intelligence

To understand the current deployment of cyber-surveillance at the municipal level, it is essential to contextualize the historical shift in American policing. In the immediate aftermath of the September 11 attacks, municipal police departments—particularly in high-profile targets like New York City and Los Angeles—were forced to rapidly redefine their operational parameters to include counter-terrorism as a primary objective. As former law enforcement executives have noted, counter-terrorism operations, which previously occupied a fractional percentage of police resources in the 1990s, suddenly consumed up to 40 percent of operational focus in major jurisdictions.

This paradigm shift necessitated the creation of regional intelligence "fusion centers" and the acquisition of military-grade hardware. However, as physical counter-terrorism infrastructure matured, the theater of threat assessment migrated to the digital sphere. Modern municipal policing is increasingly reliant on data-driven intelligence, seeking to proactively identify ideological extremism, track the organizing networks of civil dissidents, and monitor the digital footprints of local populations.

The primary challenge for local law enforcement has been the legal and technical limitations of navigating the vast expanses of the internet, the deep web, and encrypted social media ecosystems. Traditional investigative techniques requiring judicial warrants based on probable cause are often deemed too slow or restrictive for proactive threat modeling. Consequently, municipal agencies have turned to commercial off-the-shelf (COTS) cyber-surveillance solutions. Vendors specializing in artificial intelligence and automated data scraping offer police departments the ability to monitor populations at scale, utilizing algorithms to map associations, infer criminal intent, and trace physical locations without the friction of constitutional oversight. This environment has created a highly lucrative market for private cyber-intelligence firms, many of which are founded by veterans of foreign state intelligence services who bring military-grade cyber-warfare architectures to domestic civilian policing.

Foreign-State-Affiliated Cyber-Surveillance Vendors: Technical Capabilities and Controversies

The technological enforcement of the policy frameworks advocated by municipal leaders requires sophisticated infrastructure capable of processing massive, unstructured data streams. Two primary vendors—Cobwebs Technologies and Voyager Labs—have emerged as the dominant purveyors of these capabilities to U.S. municipal police departments, regional fusion centers, and district attorneys' offices. Both firms possess deep ties to the Israeli cyber-intelligence sector and offer software suites that dramatically expand the reach of local law enforcement into the private digital lives of citizens.

Cobwebs Technologies (PenLink): OSINT, Tangles, and WebLoc Geofencing

Founded in 2015 by former members of the Israeli intelligence community, Cobwebs Technologies pitches itself as an AI-powered internet monitoring service. The firm's architecture is designed to collect, analyze, and monitor data across open sources, social media, the deep web, and the dark web. In 2023, attempting to shed regulatory scrutiny and public controversy stemming from its operations, Cobwebs merged into the U.S.-based software company PenLink, rebranding its international entities (including its U.K. and German offices) to remove the "Cobwebs" name.

Cobwebs' operational capability relies on three flagship modules frequently acquired by local and federal agencies: Tangles, WebLoc, and Lynx.

- **Tangles:** This is the core web investigation platform that allows customers to conduct real-time monitoring of geo-locations, keywords, and social media profiles. Tangles utilizes automated web scrapers to bypass standard user privacy settings, aggregating information that is ostensibly public but practically obscured without advanced algorithmic collation. The U.S. Department of Homeland Security (DHS) has notably utilized Tangles to compile intelligence dossiers on domestic protesters.
- **WebLoc:** Sold as an add-on geospatial and signals intelligence platform to Tangles, WebLoc represents a significant escalation in surveillance capacity. WebLoc is marketed as a cutting-edge location solution that automatically monitors and analyzes location-based data within any specified geographic perimeter (geofencing). By analyzing Ad-ID data and mobile application telemetry—often purchased from third-party data brokers—WebLoc allows law enforcement to track the historical and real-time physical movements of devices without traditional cellular warrants.

The operational hazard of Cobwebs' software was exposed in December 2021 when Meta (the parent company of Facebook and Instagram) published its "Threat Report on the Surveillance-for-Hire Industry." Following an exhaustive investigation, Meta banned Cobwebs Technologies from its platforms, removing roughly 200 accounts operated by the firm. According to Meta's findings, Cobwebs engaged in illicit social engineering, utilizing fake accounts to trick individuals into revealing private information. Meta noted that Cobwebs' customers frequently targeted activists, opposition politicians, and government officials.

Despite this public blacklisting by the world's largest social media platform for egregious Terms of Service violations, Cobwebs (and subsequently PenLink) continued to secure lucrative contracts across U.S. jurisdictions. The Texas Department of Public Safety and the Los Angeles Police Department both signed contracts for Cobwebs' software between 2021 and 2022. Furthermore, between 2020 and 2024, the Washington D.C. Homeland Security and Emergency Management Agency (HSEMA) spent $348,613.70 to license the Tangles software specifically as "a technological tool for social media threat research capabilities in support of the District of Columbia fusion center". In New York, the Queens District Attorney entered into contracts for both Tangles and WebLoc to identify new threats and monitor targets. At the federal level, armed with a massive budget increase in 2025, U.S. Immigration and Customs Enforcement (ICE) spent over $5 million on these two surveillance systems.

The indiscriminate nature of Cobwebs' client base was further highlighted in 2023 when the firm provided its Tangles system to a private, politically motivated U.S. intelligence outfit run by religious fundamentalists who claim to hunt sex workers, thereby exposing the private information of vulnerable domestic groups to non-governmental actors.

Voyager Labs: Algorithmic Determinism and the Friendship Report

While Cobwebs focuses heavily on data aggregation and geographic telemetry, Voyager Labs

represents a highly controversial shift toward predictive behavioral analysis. Also founded by veterans of the Israeli intelligence apparatus, Voyager markets its software to municipal police departments with the bold—and scientifically dubious—claim that it can predict criminal behavior and assess the dangerousness of individuals based solely on their social media footprint. The company's core surveillance suite comprises four offerings: VoyagerInsights, VoyagerAnalytics, VoyagerVision, and VoyagerCheck.

The most invasive and discriminatory mechanism within Voyager's arsenal is the **Friendship Report**. This automated module is designed to generate a fully exportable "deep dive" into the relationship between a target account and all associated connections across social networks. The algorithm evaluates who a target's mutual friends are, the exact date the connection was established, the frequency and nature of their interactions, and provides direct links to specific interactions.

Voyager's system escalates beyond mere mapping by applying proprietary AI to assess whether an individual's online associations, ethnic heritage, or religious beliefs correlate with extremism. Internal documentation reveals that the software utilizes proxy variables, such as identifying if a user has "Arab heritage," as an indicator of dangerous extremism. Data scientists and civil liberties advocates have consistently refuted the scientific validity of these predictions, arguing that they codify racial, ideological, and religious bias into a black-box algorithm, effectively flagging people as potential criminals based on their online associations.

Voyager's illicit data harvesting methodologies prompted massive legal retaliation. In January 2023, Meta filed a federal lawsuit against Voyager Labs, alleging that the surveillance firm violated Facebook's terms of service by creating more than 38,000 fake user accounts. These synthetic identities were deployed to scrape massive troves of data—including posts, likes, friend lists, photos, and comments—from over 600,000 Facebook users. The victims of this dragnet surveillance were not limited to criminal suspects; they included employees of news organizations, nonprofits, labor unions, and government agencies, along with parents and retirees.

The marketing pitches deployed by Voyager highlight the asymmetric and opaque capabilities granted to local police. In documents obtained by the Brennan Center for Justice regarding the LAPD's four-month trial of the software in 2019, Voyager advertised its ability to provide "anonymous" and "traceless" data collection using multiple proxies to reconstruct closed and private profiles based on publicly available information.

The adoption of Voyager Labs is highly dependent on a municipality's budget size. Research indicates that larger agencies are more likely to have specialized intelligence units capable of operating these platforms. The New York Police Department (NYPD), for instance, has been a primary adopter, spending over $10.6 million since 2018 on Voyager Labs and its AI social media surveillance products. The NYPD defends the use of these tools, stating they assist in preventing victimization, though they ambiguously claim to only analyze publicly available information while simultaneously admitting to viewing data hidden behind user privacy settings—a feat achieved through the use of police-operated fake profiles.

Feature Comparison	Cobwebs Technologies (Tangles / WebLoc)	Voyager Labs (VoyagerInsights / Friendship Report)
Core Technical Capability	Real-time geo-fencing, OSINT tracking, Deep/Dark Web indexing.	Predictive AI behavioral analysis, deep social network mapping.
Signature Invasive Module	**WebLoc:** Tracks physical location via Ad-ID and mobile	**Friendship Report:** Deep-dive analysis of mutual

Feature Comparison	Cobwebs Technologies (Tangles / WebLoc)	Voyager Labs (VoyagerInsights / Friendship Report)
	telemetry signals without cellular warrants.	relationships, interaction frequency, and date of establishment.
Meta / Social Media Sanctions	Banned in 2021; Meta removed ~200 fake accounts used for social engineering.	Sued by Meta in 2023; created 38,000 fake accounts to scrape 600,000 user profiles.
Documented Municipal / Domestic Adoption	LAPD, Hartford PD, Washington D.C. HSEMA (Fusion Center), Queens DA, ICE, Texas DPS, San Joaquin County.	NYPD ($10.6M spend since 2018), LAPD (2019 trial).
Civil Liberties / Profiling Risk	Collects geo-signals around legal protests, religious centers, and targeted demographics.	Assigns "extremism" risk scores based on online associations and proxy variables (e.g., Arab heritage).

Obfuscated Procurement: Federal Subsidization via HSGP and UASI

The acquisition of million-dollar, military-grade cyber-intelligence platforms is rarely sustainable through standard municipal police operating budgets. Furthermore, presenting a line-item request for software known to have been sued by Meta for illicit surveillance would likely trigger intense public backlash from civil rights organizations and stringent scrutiny from city councils. To circumvent this friction, municipalities leverage vast federal grant pipelines, specifically the Homeland Security Grant Program (HSGP) and the Urban Area Security Initiative (UASI). By categorizing these AI surveillance tools as "counter-terrorism," "cybersecurity," or "critical infrastructure protection" assets, local authorities successfully acquire these platforms using federal tax dollars, shielding the procurement from local budgetary debate.

The Urban Area Security Initiative (UASI) Pipeline in Los Angeles

The UASI program is theoretically designed to assist high-threat, high-density urban areas in building and sustaining capabilities to prevent, protect against, mitigate, respond to, and recover from acts of terrorism. However, an exhaustive analysis of municipal UASI expenditure justification sheets reveals that these funds are routinely diverted to acquire expansive, generalized cyber-surveillance software that monitors domestic speech and association.
A definitive example of this procurement pipeline in action is documented in the Los Angeles County Board of Supervisors' agenda concerning the FY23 and FY24 UASI grant allocations. In August 2024, the Board reviewed the allocation of over $17 million in 2023 UASI funds across county departments. The Los Angeles County Sheriff's Department was allocated the lion's share, receiving nearly $10 million ($9,988,385). Included within this massive allocation—buried among requests for bomb suits, over-water survival equipment, aerial surveillance cameras, SCUBA gear, and CBRNE (Chemical, Biological, Radiological, Nuclear, and Explosive) detection equipment—was funding for the "Cobwebs Technologies Platform" and an "Investigative Analysis Platform".

Further documentation detailing the FY24 Los Angeles UASI grant explicitly outlines a $227,500 expenditure specifically for the "Cobwebs Technologies Platform". Notably, this expenditure is categorized under "Information Technology - Cyber". This demonstrates a recurring, year-over-year federal subsidization of a platform that had already been banned by Meta for illicit domestic surveillance activities. By nesting the acquisition of social media scraping tools within a broader portfolio of traditional physical security apparatuses, law enforcement agencies effectively neutralize legislative oversight.

Cooperative Purchasing Organizations and Sole-Source Justifications

The procurement of these platforms often bypasses the standard municipal competitive bidding processes through the utilization of "sole-source" justifications or via massive, overarching IT vendor contracts. A sole-source procurement asserts that only one specific vendor can fulfill the technical requirements of the agency, eliminating the need to solicit alternative bids.
For example, public records indicate that the State Homeland Security Grant Program (SHSGP) funded the acquisition of Cobwebs Technologies for San Joaquin County via a sole-source process. Documents from this transaction reveal the direct interaction between the foreign-based software firm and the federal grant compliance bureaucracy. On December 4, 2023, Charlie Stone, the Vice President of Sales for Cobwebs Technologies, completed and signed a Byrd Anti-Lobbying Amendment certification, affirming that no federal appropriated funds were paid to influence members of Congress—a prerequisite for all federally funded procurements exceeding $100,000.
When sole-source justifications are deemed too politically risky, municipalities utilize massive cooperative purchasing organizations, such as OMNIA Partners, to acquire the software. Vendors such as Carahsoft Technology Corp act as master distributors, listing hundreds of software products on a single cooperative contract. Under the Carahsoft OMNIA contract (R240303), Voyager Labs is listed alongside mainstream IT solutions like Adobe, AWS, and Docusign. The contract explicitly notes that these solutions are applicable for purchases using the Homeland Security Grant Program, the Urban Area Security Initiative, the Transit Security Grant Program, and the Port Security Grant Program. This layered procurement methodology allows municipal leaders and police chiefs to acquire un-audited, algorithmically deterministic surveillance tools simply by purchasing off a pre-approved master list, ensuring that a specific "Voyager Labs" line-item never has to be independently debated by the city council.

The Political Vanguard: The Combat Antisemitism Movement (CAM) and Municipal Capture

The technological infrastructure provided by firms like Cobwebs and Voyager, and the funding provided by UASI, require a cohesive policy directive to dictate how these tools are deployed domestically. This is where the Combat Antisemitism Movement (CAM) operates as the strategic vanguard, providing the ideological and bureaucratic framework required to justify the massive expansion of local intelligence gathering.

Philanthropic Origins and the Mayors Advisory Board

CAM describes itself as a global coalition uniting over 950 partner organizations and hundreds of thousands of individuals to fight antisemitism in all its forms. Operating under the umbrella of

the Combat Hate Foundation, CAM was founded and heavily subsidized by Midwest oil and gas magnate, philanthropist, and Republican Party donor Adam Beren. The organization is sustained by massive capital injections from entities like the Vine & Fig Tree Fund, which has provided hundreds of thousands of dollars in grants specifically for programs combating hate and developing truth databases.

Recognizing that municipal governments—particularly mayoral offices—exert direct executive control over local police departments, emergency management agencies, and city-wide technological deployments, CAM strategically pivoted its lobbying efforts toward local governance. In October 2025, CAM officially launched its Mayors Advisory Board, designed to formulate a united front of local officials across North America.

The inaugural board is chaired by Mayor Brett Smiley of Providence, Rhode Island. It features a diverse, multi-city coalition of influential municipal leaders, including:

- Mayor Margaret Brown (Weston, FL)
- Mayor Alix Desulme (North Miami, FL)
- Mayor Marcus Muhammad (Benton Harbor, MI)
- Mayor Sharona Nazarian (Beverly Hills, CA)
- Mayor Rusty Paul (Sandy Springs, GA)
- Mayor Larisa Svechin (Sunny Isles Beach, FL)
- Mayor Howard Weinberg (Aventura, FL)
- Mayor Vince Williams (Union City, GA)

This effort was subsequently expanded in May 2026 with the launch of the Jewish Mayors and Municipal Leaders Association (JMMLA), chaired by Miami Beach Mayor Steven Meiner. The JMMLA functions as a specialized peer-exchange network intended to coordinate action on local public safety, the prevention of extremism, and high-integrity governance.

The Municipal Antisemitism Action Index: Codifying Algorithmic Parameters

The primary operational objective of the Mayors Advisory Board and the JMMLA is to advance the implementation of the **Municipal Antisemitism Action Index**. Developed by CAM, the Action Index serves as a strategic framework and practical blueprint for city-level policies, operating as the organization's signature mechanism for reshaping local law enforcement priorities.

A structural analysis of the Municipal Antisemitism Action Index reveals a heavy emphasis on the rapid expansion of intelligence-gathering capabilities and the standardization of legal definitions at the local level. The Index explicitly dictates action steps across four areas, with the most critical mandates falling under Legislation/Policy and Law Enforcement:

1. **Adoption of the IHRA Definition:** The Index mandates that municipalities integrate the International Holocaust Remembrance Alliance (IHRA) Working Definition of Antisemitism into city code and hate crime legislation. Thus far, CAM's lobbying has successfully pushed 37 to 38 U.S. states to adopt this definition.
2. **Expanded Policing Powers:** The Index calls for the implementation of "Bubble Zone Legislation" to restrict protests near sensitive areas, and "Anti-Masking Legislation" to prohibit individuals from wearing masks at public protests, directly enhancing the efficacy of municipal facial recognition systems.
3. **Establishment of Intelligence Task Forces:** Municipalities are instructed to form dedicated task forces comprising law enforcement and local leadership to transparently

report on hate incidents.
4. **Mandatory Syndication of Intelligence:** Most critically, step 4.5 of the Index explicitly mandates that local police and municipal governments must "Collect and share aggregated data on antisemitic incidents (including frequency, type, and location) with the public and CAM's Antisemitism Research Center (ARC)".

By pushing municipalities to legally codify the IHRA definition, CAM effectively broadens the scope of what constitutes an actionable threat, establishing a standardized linguistic and legal parameter for local law enforcement. This has direct technological implications. When police departments integrate the IHRA definition into their cyber-surveillance search parameters, AI tools like Cobwebs' Tangles and Voyager Labs' VoyagerInsights are explicitly programmed to crawl social media and digital spaces for keywords and associations that align with these broad policy definitions. Consequently, political advocacy at the mayoral level seamlessly translates into the algorithmic parameters of local police surveillance.

Case Studies in Municipal Surveillance Implementation

The abstract policy advocacy of CAM's Mayors Advisory Board and the federal funding mechanisms of UASI converge at the local municipal level. The actions of the mayors involved in CAM's leadership illustrate a distinct pattern: a rhetorical commitment to combating hate, operationalized through the dramatic expansion of municipal surveillance infrastructure and intelligence fusion centers.

Providence, Rhode Island: Brett Smiley and the Real-Time Crime Center

Mayor Brett Smiley of Providence, Rhode Island, serves as the inaugural Chair of CAM's Mayors Advisory Board. Under his executive leadership, the city has aggressively pursued a data-driven policing model that heavily relies on centralized technological monitoring. In August 2024, Mayor Smiley and Police Chief Oscar Perez announced the launch of Rhode Island's first Real-Time Crime Center (RTCC), a state-of-the-art operations hub funded by a $1 million federal earmark secured by U.S. Senator Jack Reed.

The Providence RTCC is designed to enhance public safety through real-time data sharing and advanced analytics, integrating live camera feeds, license plate readers, and 911 call data. To expand the surveillance net, the city actively solicits private businesses and citizens to voluntarily register and integrate their private security cameras directly into the police network, effectively crowdsourcing a city-wide panopticon.

While Mayor Smiley's administration insists the RTCC incorporates strict oversight policies, data retention limits, and usage auditing, civil liberties organizations have aggressively contested these claims. In August 2024, the ACLU of Rhode Island issued a public letter to Mayor Smiley denouncing the center as an "all-encompassing surveillance system," specifically citing that after reviewing the center's standard operating procedures, it was determined that the RTCC "possesses no semblance of a meaningful privacy policy". The ACLU had previously warned that the Providence Police Department was intent on creating a "mini-surveillance state" capable of spying on citizens without sufficient legislative oversight or data-gathering transparency.

As the Chair of CAM's Mayors Advisory Board, Smiley's commitment to building the RTCC reflects the technological imperative embedded in the Municipal Antisemitism Action Index—establishing the physical and digital infrastructure necessary to continuously monitor the local populace, thereby ensuring that rapid intelligence aggregation is available to municipal authorities to track ideological incidents.

North Miami, Florida: Alix Desulme’s Panoptic Expansion

Mayor Alix Desulme of North Miami, another prominent member of the CAM Mayors Advisory Board, has similarly prioritized the expansion of digital surveillance. Desulme is recognized by CAM for his visible, principled leadership, which earned him the CAM Mayors of Courage Award at the 2025 North American Mayors Summit Against Antisemitism.

In response to local security concerns, Desulme has championed initiatives to increase police patrols and radically enhance technological monitoring. Municipal records indicate consistent support for resolutions authorizing the installation of license plate recognition (LPR) cameras and video surveillance equipment across special taxing districts within the city, with the local government collecting special assessments to fund the improvements. Pushing the boundary of public-private surveillance integration, the North Miami Community Redevelopment Agency (CRA) approved the direct distribution of commercial surveillance cameras (such as Ring and Blink devices) to residents. This initiative expands the overall footprint of monitored areas, creating a localized network of privatized cameras that can readily feed data back into municipal and law enforcement oversight systems.

The Atlanta Suburbs: Regional Mayoral Roundtables

The expansion of CAM's influence is evident in its regional organizing, notably within the Atlanta, Georgia suburbs. Mayors Rusty Paul of Sandy Springs and Vince Williams of Union City—both members of the CAM Mayors Advisory Board—have utilized their platforms to advocate for municipal-level intervention against hate. In January 2026, the Georgia Mayors Roundtable on Antisemitism convened at the Sandy Springs City Hall to coordinate collaborative forums. Mayor Williams explicitly noted that mayors possess an "unbelievable" platform to lead and bring solace to communities by stopping hate.

This regional coordination mirrors CAM's broader law enforcement initiatives in the state. CAM has previously hosted law enforcement training forums where more than 80 police officers from across Georgia were trained to identify "antisemitic extremism". By simultaneously organizing the political executives (mayors) and training the operational enforcers (police), CAM ensures that the ideological parameters defining extremism are uniformly adopted across regional municipal infrastructures, paving the way for the deployment of surveillance tools calibrated to these specific definitions.

Washington D.C. and New York City: The Fusion Center Nexus

In major metropolitan areas, the scale of surveillance procurement is exponentially larger. Between 2020 and 2024, the Washington D.C. Homeland Security and Emergency Management Agency (HSEMA) spent nearly $350,000 to license Cobwebs' Tangles software to support the District of Columbia fusion center's threat research capabilities. The ACLU of D.C. filed Freedom of Information Act requests demanding transparency, noting the substantial risk of abuse when the government utilizes technology to track people's speech and movements.

In New York City, under the administration of Mayor Eric Adams—a frequent keynote speaker at CAM summits who recently launched a citywide Office to Combat Antisemitism —the NYPD has operated as a massive consumer of Voyager Labs' technology. The NYPD has spent over $10.6 million on Voyager's AI social media surveillance products since 2018 , while the Queens District Attorney has actively contracted with Cobwebs for Tangles and WebLoc.

Municipal Leader / City	Role in CAM Ecosystem	Key Surveillance / Intelligence Implementations
Mayor Brett Smiley (Providence, RI)	Chair, Mayors Advisory Board	Launched $1M Real-Time Crime Center (RTCC); integration of live private/public camera feeds. Criticized by ACLU for lacking privacy policies.
Mayor Alix Desulme (North Miami, FL)	Member, Mayors Advisory Board	Distributed Ring/Blink cameras to residents via CRA; expanded License Plate Recognition networks.
Mayor Eric Adams (New York, NY)	Keynote Speaker, CAM Summits	NYPD spends $10.6M on Voyager Labs; Queens DA contracts Cobwebs; launched Office to Combat Antisemitism.
D.C. HSEMA (Washington, D.C.)	Fusion Center Hub	Procured Cobwebs Tangles for $348k to conduct social media threat research.

The Data Syndication Pipeline: ARC and the Privatization of Intelligence

The most alarming aspect of this municipal surveillance ecosystem is not merely the collection of localized data, but its subsequent syndication, aggregation, and weaponization. The critical endpoint of the commercial procurement pipelines established by Cobwebs and Voyager is the transfer of actionable intelligence from publicly funded law enforcement agencies to private, ideological data repositories—specifically, the Antisemitism Research Center (ARC), managed by the Combat Antisemitism Movement.

The Antisemitism Research Center (ARC)

The Antisemitism Research Center (ARC) serves as CAM's proprietary global intelligence hub. It utilizes specialized methodologies to comprehensively track, aggregate, and analyze antisemitic trends and incidents worldwide. ARC publishes detailed weekly, monthly, and annual reports that categorize incidents by ideology (e.g., Islamist, far-right, far-left), motivation, and manifestation. The scale of ARC's data aggregation is immense; in 2024, ARC documented an alarming 6,326 antisemitic incidents globally, representing a staggering 107.7% increase from 2023, and tracked a 300% increase in incidents specifically on U.S. college campuses.
ARC does not rely solely on passive community reporting; it actively monitors the digital sphere. The center conducts sophisticated analyses of social media algorithms, utilizing independent researchers and AI tools to track how platforms expose users to content. In March, ARC

published the "Engineered Exposure" report, which documented how Instagram's recommendation engine algorithmically pushed antisemitic content to neutral users, generating millions of views without the users actively searching for it. ARC's tracking capabilities are sophisticated enough to document specific regional violence, identify the ideological affiliation of perpetrators, and even track complex terror plots orchestrated by foreign entities like Iran's Islamic Revolutionary Guard Corps (IRGC) targeting diplomatic pipelines.

The API Handshake: Fusing Public Surveillance with Private Repositories

The critical operational connection between local police departments and the ARC database is established through the mandatory policy directives of the CAM Mayors Advisory Board. As detailed previously, Step 4.5 of CAM's Municipal Antisemitism Action Index explicitly mandates that local governments must "collect and share aggregated data on antisemitic incidents... with the public and CAM's Antisemitism Research Center (ARC)".

This directive establishes a direct, privatized intelligence pipeline. The operational workflow functions as follows:

1. **Federal Funding & Procurement:** A municipality utilizes UASI or HSGP grants to acquire advanced OSINT tools like Cobwebs' Tangles or Voyager Labs, funneling the purchase through cooperative vehicles like OMNIA to avoid local scrutiny.
2. **Algorithmic Parameter Setting:** The Mayor ensures the local police department has adopted the IHRA definition of antisemitism into city code, expanding the parameters of what constitutes a trackable threat.
3. **Data Harvesting:** Local intelligence analysts or fusion centers deploy WebLoc to geofence protests or utilize Voyager's Friendship Report to map the social networks of activists based on the newly expanded keyword parameters.
4. **Data Syndication:** The resulting localized intelligence—profiles of protesters, social network maps, demographic tracking, and incident reports—is aggregated. Following the mandate of the Municipal Action Index, this data is formatted and syndicated directly into the ARC database. This is achieved through automated API (Application Programming Interface) handshakes or formalized data-sharing agreements that connect municipal incident databases to ARC's global tracking matrix.

This data funnel represents the wholesale privatization of state-gathered intelligence. By sharing police-gathered data with ARC, local municipalities are effectively transferring intelligence—collected under the guise of public safety using federally subsidized, privacy-violating cyber-tools—into a private database that operates outside the boundaries of the Freedom of Information Act (FOIA), constitutional oversight, and local electoral accountability.

Once housed within ARC, this localized data is repackaged into alarming, macro-level statistical reports. These reports are then distributed back to federal lawmakers, state legislatures, and municipal leaders to justify the procurement of even more funding and advanced surveillance technologies, creating a self-sustaining, closed-loop military-industrial-municipal complex. CAM executives explicitly leverage this data at forums, such as the National Sheriffs' Association, to call for deeper law enforcement collaboration and to investigate the entities "facilitating the mayhem". Furthermore, CAM recently partnered with *The Jerusalem Post* to launch a global antisemitism monitoring portal, ensuring this privatized intelligence is broadcast to international

policymakers to implement targeted responses.

The Operational Blurring of Protest, Vandalism, and Terror

The danger of this syndication pipeline is acutely visible when examining how ARC categorizes and utilizes the data it receives. ARC tracking systems explicitly map online behavior, tracking pro-Palestinian organizations, campus protests, and digital anti-Israel sentiment alongside legitimate terror threats. Through tools like Tangles and Voyager, local police are equipped to deanonymize these protesters and map their relationships.

When a protest group engages in civil disobedience or disruptive actions, the fusion of local police data and ARC's global tracking matrix allows for rapid ideological classification and political weaponization. For instance, when members of the activist group Palestine Action infiltrated a Royal Air Force base to vandalize Voyager aircraft with red paint, the British government—spurred by advocacy from groups tracking this data—moved to ban Palestine Action under anti-terrorism laws, classifying them alongside ISIS and al-Qaeda. By funneling domestic protest data through Israeli-affiliated algorithms and into a private database managed by an organization with explicit geopolitical objectives, U.S. municipal police departments are inadvertently operating as domestic intelligence-gathering nodes for a highly politicized, international policy apparatus.

Algorithmic Bias and the Erasure of Civil Liberties

The convergence of UASI grant funding, foreign AI surveillance vendors, and the political advocacy of the Combat Antisemitism Movement creates severe, structural threats to American civil liberties.

The Erosion of First and Fourth Amendment Protections

The reliance on tools like Cobwebs Technologies and Voyager Labs fundamentally subverts the Fourth Amendment's protection against unreasonable search and seizure. By purchasing access to massive repositories of scraped social media data, location telemetry, and reconstructed private profiles—often via fake accounts—law enforcement bypasses the judicial requirement to obtain a warrant based on probable cause. The use of WebLoc to track the historical movements of individuals via Ad-ID data essentially achieves the results of a wiretap or a GPS tracker without the requisite judicial oversight, enabling dragnet surveillance of entire neighborhoods or protest zones.

Furthermore, the deployment of predictive policing tools like Voyager's Friendship Report exerts a profound chilling effect on First Amendment rights to free speech and free association. If citizens know that local law enforcement is mapping their online interactions to assign them an "extremism" score based on their religious heritage, political posts, or mutual friends , they are fundamentally deterred from engaging in political discourse or participating in legal protests.

The Weaponization of the IHRA Definition in Algorithmic Targeting

The adoption of the IHRA definition of antisemitism into the cyber-search parameters of police departments effectively programs political and ideological bias into the surveillance algorithm. Critics have forcefully argued in legislative testimonies that the IHRA working definition is

routinely utilized to police how individuals speak, write, and converse about the State of Israel, conflating political criticism of a state with ethnic hatred.
Data scientists have repeatedly warned that artificial intelligence systems designed to gauge "criminal intent" are inherently flawed and act as laundering mechanisms for existing institutional biases. When a mayor, guided by CAM's advisory board and the Municipal Action Index, instructs a police department to utilize Voyager Labs to root out hate crimes based on the IHRA definition, the software will inevitably target and surveil marginalized communities, pro-Palestinian activists, and specific religious demographics based on the proxy indicators built into its code. The system does not merely observe; it mathematically determinates guilt by association.

Synthesis and Strategic Outlook

The commercial procurement pipelines integrating foreign-state-affiliated cyber-surveillance systems into U.S. municipal police departments are neither accidental nor purely market-driven. They are the result of a meticulously engineered, politically motivated policy architecture. The Combat Antisemitism Movement, utilizing the executive authority of its Mayors Advisory Board and the structured mandates of the Municipal Antisemitism Action Index, provides the ideological and bureaucratic framework required to justify the massive expansion of local intelligence gathering under the guise of public safety.
Simultaneously, the federal government, through the opaque, highly lucrative, and easily obfuscated channels of the UASI and HSGP grant programs, provides the unchecked financial capital necessary to acquire elite cyber-weapons from controversial vendors like Cobwebs Technologies and Voyager Labs. These tools grant municipal police the capability to conduct warrantless tracking and predictive profiling, capabilities that have resulted in major lawsuits and bans from primary technology platforms like Meta.
Finally, the localized data harvested by these algorithmic dragnets is siphoned back up through mandated reporting APIs into CAM's private Antisemitism Research Center (ARC) database. This creates a shadow repository of domestic intelligence, fusing state surveillance power with private geopolitical advocacy, entirely immune to the transparency laws that govern public agencies. Until legislative bodies enforce strict auditing of UASI grant expenditures, prohibit sole-source procurement of COTS surveillance tools, and ban the municipal acquisition of algorithmic tracking platforms that inherently violate platform terms of service and bypass constitutional warrants, local city halls will continue to function as the operational front lines for an unchecked, privatized surveillance state.

Works cited

1. 20 Years Later - Police Chief Magazine, https://www.policechiefmagazine.org/wp-content/uploads/Police_Chief_Sept2021.pdf 2. Cobwebs Technologies Careers, Jobs, and Salary Information, https://www.theladders.com/company/cobwebstechnologies-jobs 3. 1 Via Public FOIA Portal August 7, 2025 Joe Ruel FOIA Officer District of Columbia Homeland Security and Emergency Management Ag - ACLU of DC, https://www.acludc.org/app/uploads/2025/08/8.5.2025-FOIA-Request-Cobwebs.pdf 4. Comments to the Federal Trade Commission re: Commercial Surveillance ANPR, R111004 submitted by: The Brennan Center for Justice,

https://www.brennancenter.org/media/10569/download/Brennan%20Center%20FTC%20Comment_1.pdf?inline=1 5. Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech,
https://citizenlab.ca/research/analysis-of-penlinks-ad-based-geolocation-surveillance-tech/ 6. Is Webloc Coming to Your Neighborhood?,
https://godarkbags.com/blogs/post/is-webloc-coming-to-your-neighborhood 7. ACLU-D.C. Files FOIA Request on the District's Use of Web-Based Surveillance Software that Can Track People's Speech and Movements,
https://www.acludc.org/press-releases/aclu-d-c-files-foia-request-on-the-districts-use-of-web-based-surveillance-software-that-can-track-peoples-speech-and-movements/ 8. 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 9. Aimed at Protests, Surveillance Contractor's New Owners Expand Spy Tech Portfolio,
https://unicornriot.ninja/2023/aimed-at-protests-surveillance-contractors-new-owners-expand-spy-tech-portfolio/ 10. 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 11. 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 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. Social Media Intelligence: Responding to Crime and Violence in the Digital World,
https://repository.rit.edu/cgi/viewcontent.cgi?article=13193&context=theses 14. Public Safety Cluster Agenda Review Meeting - Lacounty,
https://file.lacounty.gov/SDSInter/ceo/agendas/1165111_2024.08.07AgendaandDocs.pdf 15. 2024 Urban Areas Security Initiative (UASI) Grant Award ... - City Clerk,
https://cityclerk.lacity.org/onlinedocs/2024/24-0975_rpt_mayor_3-19-25.pdf 16. OFFICE OF THE COUNTY COUNSEL,
https://www.eff.org/files/2024/12/18/redacted_documents_response_110824_0.pdf 17. Contract # for with Effective: - OMNIA Partners,
https://www.omniapartners.com/suppliers-files/A-D/Carahsoft_Technology_Corp/Contract_Documents/R240303/R240303_Carahsoft_MAD.pdf 18. Combat Antisemitism Movement Names New US Advisory Board Members and Chair,
https://combatantisemitism.org/press-release/combat-antisemitism-movement-names-new-us-advisory-board-members-and-chair/ 19. Mayors Form New Multi-City Board to Fight Antisemitism | Combat ...,
https://combatantisemitism.org/press-release/mayors-form-new-multi-city-board-to-fight-antisemitism/ 20. Combat Hate Foundation - Influence Watch,
https://www.influencewatch.org/non-profit/combat-hate-foundation/ 21. Philos Project - Influence Watch, https://www.influencewatch.org/non-profit/philos-project/ 22. report of 2024-2025 - grants awarded - UJA-Federation, https://www.ujafedny.org/api/v2/assets/Grants-Book-2025.pdf 23. North Miami Mayor Appointed to National Board to Fight Antisemitism,

http://www.northmiamifl.gov/m/newsflash/Home/Detail/442 24. Jewish Mayors and Municipal Leaders Association Launches at Miami Beach Event, https://combatantisemitism.org/government-and-policy/a-significant-and-distinct-voice-in-american-city-life-cam-unveils-jewish-mayors-and-municipal-leaders-association-at-miami-beach-launch-event/ 25. Combat Antisemitism Movement Launches Jewish Mayors and Municipal Leaders Association, https://combatantisemitism.org/press-release/combat-antisemitism-movement-launches-jewish-mayors-and-municipal-leaders-association/ 26. CAM Antisemitism Research Center Database of IHRA Definition Adoptions by US States, https://combatantisemitism.org/government-and-policy/cam-information-hub-database-of-ihra-antisemitism-definition-adoptions-by-us-states-2/ 27. Antisemitism Legislation Advances in Three States as Part of Nationwide Effort to Combat Rising Jew-Hatred, https://combatantisemitism.org/government-and-policy/antisemitism-legislation-advances-in-three-states-as-part-of-nationwide-effort-to-combat-rising-jew-hatred/ 28. Proponent of SB 87 David Soffer Combat Antisemitism Movement (CAM) Good afternoon, Chairman Manning and esteemed Members of the, https://search-prod.lis.state.oh.us/api/v2/general_assembly_136/committees/cmte_s_judiciary_1/meetings/cmte_s_judiciary_1_2026-02-11-0945_1022/testimony/13717/oh_sb_87_testimony_2_10.pdf 29. News Flash - North Miami, FL, https://www.northmiamifl.gov/1625/Press-Releases 30. Mayor Brett Smiley and Colonel Oscar Perez Announce Launch of Real Time Crime Center - City of Providence, https://www.providenceri.gov/mayor-brett-smiley-and-colonel-oscar-perez-announce-launch-of-real-time-crime-center/ 31. New city crime center draws criticism from anti-surveillance advocates, https://www.browndailyherald.com/article/2025/09/new-city-crime-center-draws-criticism-from-anti-surveillance-advocates 32. Smiley Under Pressure, Unveils “Real-Time Crime Center” Initiated by Elorza - GoLocalProv, https://www.golocalprov.com/news/smiley-under-pressure-unveils-real-time-crime-center-initiated-by-elorza 33. Alix Desulme to be honored at North American Mayors Summit Against Antisemitism - Florida Politics, https://floridapolitics.com/archives/767430-alix-desulme-to-be-honored-at-north-american-mayors-summit-against-antisemitism/ 34. Councilman - Alix Desulme,Ed.D. - North Miami, FL, https://www.northmiamifl.gov/Archive.aspx?ADID=174 35. resolution of the mayor and city council of - North Miami, FL, https://www.northmiamifl.gov/DocumentCenter/View/2349/Resolution-2018-135--10-23-2018-PDF 36. Atlanta Area Mayors Convene for Collaborative Forum on Municipal-Level Fight Against Antisemitism, https://combatantisemitism.org/government-and-policy/atlanta-area-mayors-convene-for-collaborative-forum-on-municipal-level-fight-against-antisemitism/ 37. 'Your Jewish Community Is Scared': At National Sheriffs' Association Forum, CAM Calls for Law Enforcement Collaboration in Antisemitism Fight, https://combatantisemitism.org/cam-news/your-jewish-community-is-scared-at-national-sheriffs-association-forum-cam-calls-for-law-enforcement-collaboration-in-antisemitism-fight/ 38. 'It's Not Just About One, It's About All': City Leaders From Across North America Convene in New Orleans for United Action Against Antisemitism, https://combatantisemitism.org/cam-news/its-not-just-about-one-its-about-all-city-leaders-from-across-north-america-convene-in-new-orleans-for-united-action-against-antisemitism/ 39. Eye on Extremism: July 18, 2025,

https://www.counterextremism.com/roundup/eye-extremism-july-18-2025 40. CAM Antisemitism Research Center Monthly Report January 2024, https://25352948.fs1.hubspotusercontent-eu1.net/hubfs/25352948/CAM%20Antisemitism%20Research%20Center%20Monthly%20Report%20January%202024.pdf?utm_medium=email&_hsmi=82484367&_hsenc=p2ANqtz-8lY_hxpOEMjZ_nok4DLKPv392eRFoAboS5v1zmINI6EwDSYfrbW5Yn5vzbsBEoXiClpVQc0qVECzGbFcRbsr8W2KJyEw&utm_content=82484367&utm_source=hs_email 41. research center - Combat Antisemitism Movement, https://combatantisemitism.org/research/ 42. Data on Antisemitism, https://combatantisemitism.org/data-on-antisemitism/ 43. Islamists Drove 80% of Ideologically-Motivated Antisemitic Violence in April, CAM Data Shows, https://combatantisemitism.org/studies-reports/islamists-drove-80-of-ideologically-motivated-antisemitic-violence-in-april-cam-data-shows/ 44. Ron Tusler - Wisconsin Legislative Documents, https://docs.legis.wisconsin.gov/misc/lc/hearing_testimony_and_materials/2025/ab446/ab0446_2025_10_22.pdf 45. Combat Antisemitism Movement, https://combatantisemitism.org/ 46. Opinion: The Data Makes it Undeniable: Facebook is Suppressing Jewish Voices, https://www.jewishtimes.com/the-data-makes-it-undeniable-facebook-is-suppressing-jewish-voices/ 47. Iran-Linked Hackers Offer Cash Bounties on Israeli Air Defense Engineers, https://combatantisemitism.org/cam-news/iran-linked-hackers-offer-cash-bounties-on-israeli-air-defense-engineers/ 48. Weekly Report - March 12, 2026 | Combat Antisemitism Movement, https://combatantisemitism.org/newsletters/weekly-report-march-12-2026/ 49. Antisemitism in Italy in 2024 – The Annual Report of the CDEC Foundation's Observatory - AWS, https://wjc-org-website.s3.amazonaws.com/horizon/assets/z5g5bPE7/annual_report_on_antisemitism-2024-ita.pdf 50. The Chicago Community Trust - Form 990, Schedule I - Nonprofit Explorer - ProPublica, https://projects.propublica.org/nonprofits/organizations/362167000/202312279349301591/IRS990ScheduleI 51. CAM and The Jerusalem Post Launch Global Antisemitism Monitoring Portal to Combat Rising Hate, https://combatantisemitism.org/cam-news/cam-and-jerusalem-post-launch-global-antisemitism-monitoring-portal-to-combat-rising-hate/ 52. Anti-Israel Campus Groups: Online Networks & Narratives - Institute for the Study of Contemporary Antisemitism, https://isca.indiana.edu/publication-research/social-media-project/current-projects/anti-israel-campus-groups-draft.html 53. Activists are exploiting Western values defending pro-Palestine orgs | The Jerusalem Post, https://www.jpost.com/diaspora/antisemitism/article-859968 54. UK to Ban Palestine Action as Terrorist Group After RAF Base Sabotage, Violent Protests, https://combatantisemitism.org/cam-news/uk-to-ban-palestine-action-as-terrorist-group-after-raf-base-sabotage-violent-protests/