THE LEGAL INVESTIGATOR

Journal of the
NATIONAL ASSOCIATION OF
LEGAL INVESTIGATORS



PATTERNS OF LIFE CAPTURED IN DATA – AND FRAUD

JASON DUMAS INVENTED A NATIONWIDE SURVEILLANCE SYSTEM. THEN HE MOTORED INTO THE PACIFIC OCEAN AND VANISHED.

BY LAEL HENTERLY, CLI - PG 8

SPRING 2026

AN OFFICIAL PUBLICATION OF THE NATIONAL ASSOCIATION OF LEGAL INVESTIGATORS, INC.



Patterns of Life captured in data – and fraud

Jason Dumas invented a nationwide surveillance system. Then he motored into the Pacific Ocean and vanished.

By Lael Henterly, CLI

A hundred years ago, what Jason Dumas did for a living would have been indistinguishable from witchcraft.

To anyone alive in 1925, the air was empty. The idea that it was dense with invisible transmission — that voices, music, and encoded data were passing through your body at the speed of light, through walls and moving vehicles, through the dark interior of your own skull — belonged to scientists and, at the fringes, mystics. Marconi had barely proved it was possible. Most people hadn't accepted that it was real.

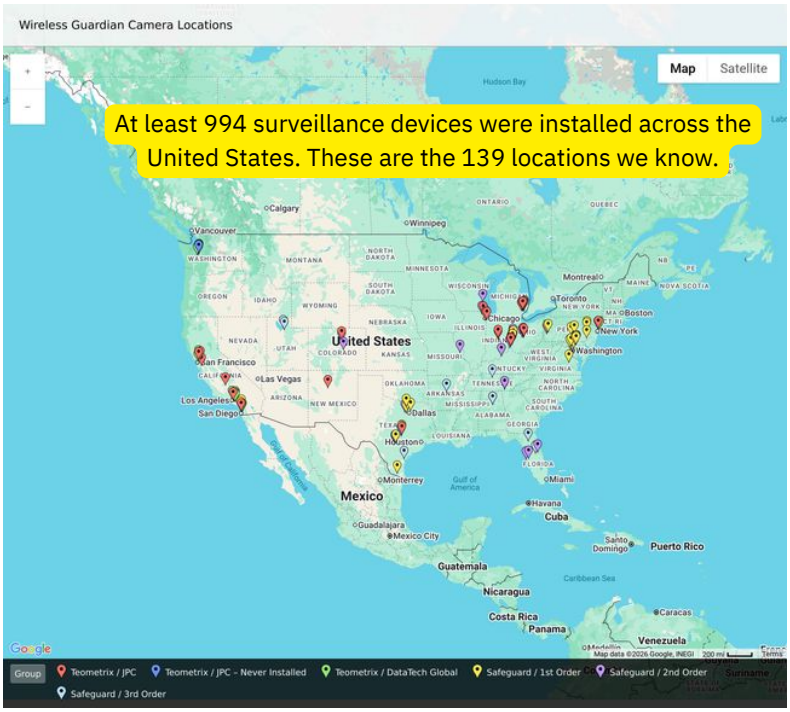
Today, everyone carries a radio. Your phone is a radio, broadcasting continuously, announcing its presence to every antenna within range. It emits a unique hardware identifier — a MAC address, burned into the chip at manufacture. It pings cellular towers. It hunts for Wi-Fi networks, advertising itself in the search. All of it is automatic, without your instruction or awareness. The phone doesn't know who's listening.

This is the raw material of SIGINT. The geometry is simple: One antenna detects a signal. Three triangulate positions. With enough receivers, you resolve a specific device — and therefore its owner within one square meter. You track their movement as the phone hands off between antennas like a baton between runners. You cross-reference the extracted identity against a watch list.

Jason Dumas spent 20 years as a radio frequency engineer, developing a feel for this invisible world. He liked to tell the story of how he overhauled the White House wireless infrastructure so Obama could keep his BlackBerry. He wired stadiums — the Superdome, Ford Field, JFK, the Smithsonian — building the distributed antenna systems that hold 70,000 phones coherent in an overloaded spectrum. In doing so, he learned to read a crowd as signals: nodes moving through space, each trailing an electromagnetic signature as legible, to the right instruments, as a face.

By 2018, he had refined that knowledge into two patents on a data collection box he'd later call Sentinel. By 2022, he was selling investors on a network of rooftop antennas at gas stations, truck stops, and budget motels across 43 states — each one harvesting the identity of every phone that passed beneath it.

He told investors the data would allow businesses to display targeted ads to customers. He asked Labyrinth Technologies to design a signals intelligence box.



THE SCHEME

Dumas and Dwayne Ratliff founded Wireless Guardian to blanket America's highways with surveillance equipment — a choke-point network, quietly wired to rooftops along the nation's arterials, sled-mounted so no permits were required.

To build a nationwide surveillance network, you must first build the network. To finance that construction — patented technology, custom hardware, cloud infrastructure — you need capital. However, Dumas and Ratliff were, by conventional measures, not creditworthy. Ratliff emerged from a Chapter 7 bankruptcy filed in December 2012, listing personal guarantees totaling more than $30 million for six collapsed real estate projects. Dumas carried a past marred by bad checks, theft, and litigation alleging he stole a business partner's company — a 2016 suit that traced a pattern familiar to those who later lost money to Wireless Guardian. Neither man attracted institutional money. Instead, they relied on personal relationships and a pyramid of resellers worthy of a multilevel marketing scheme.

The pitch found ordinary investors where hope lives: in the promise of passive income. *Buy a box. We will install it on your roof. It captures behavioral data from passing traffic. Intel Corporation purchases that data. You collect a monthly revenue share. Guaranteed.*

The Boxes

The tech was real. Manufactured by Xanthon — formerly Labyrinth Technologies, a St. Louis company — engineering drawings filed inadvertently in a contract dispute and dated April 2020 describe four antenna channels on 10-foot extension cables: two Wi-Fi MIMO elements, one Bluetooth, and one labeled by drafting engineer Frank Bryant with two words that don't appear in advertising technology specifications: SigInt Antenna.



Signals intelligence. The purview of the NSA. Of spies. Deployed by soldiers in combat zones to target enemies. An antenna designed to collect IMSI data.

Labyrinth-sourced components through a supply chain routed through GetWireless, a Minnesota IoT distributor whose catalog — Sierra Wireless AirLink routers, Panorama multi-function antennas — screams law enforcement. Data is uploaded in near real time to a cloud infrastructure with a Department of Defense–sponsored FedRAMP authorization. Wireless Guardian's own marketing noted that law enforcement could access it for investigative analysis. This was never an advertising technology stack.



Can Legal Investigators Access the Data Trove?

PatternView is soliciting buyers. A licensed firm with a plausible institutional need — insurance, asset recovery, corporate due diligence — can respond to that solicitation and see what terms are offered. Attempts to reach PatternView were unsuccessful. A contact form promised a confirmation email that never arrived. The privacy and compliance page says: Coming Soon. Make of that what you will. A note on what you'd be buying regardless: data collected by a network that may have operated in violation of federal wiretapping statutes, the Electronic Communications Privacy Act, and FCC licensing rules is not clean data. Its admissibility would likely be contested. Caveat emptor.

For cleaner location data — SDK-sourced, drawn from consumers who agreed, however unwittingly, to share their location in exchange for a free flashlight app — the commercial market is open for business.

Babel Street and **Creative Radicals** are the accessible retail counter: sales teams, compliance frameworks, interfaces built for professionals who want answers without building anything.

The upstream well is **Venntel**, whose confirmed government clients have included the IRS, DHS, ICE, CBP, DEA, and FBI. The factory is **Unacast**, which acquired Gravy Analytics — though the FTC hit Gravy with a final enforcement order in January 2025 over the sale of sensitive location data, including visits to medical facilities, places of worship, and political rallies. The order constrains what Gravy and its subsidiaries can sell and to whom. Due diligence before engaging.

For occasional lookups, the retail counter is fine. For a long-running matter with geographic complexity — a subject's pattern of life across months and multiple states — going direct is worth the conversation. The FBI is still having it. Director Kash Patel confirmed as recently as March 2026 that the bureau purchases commercially available location data, calling it consistent with the Constitution. Senator Ron Wyden called it an outrageous end-run around the Fourth Amendment.

Both of them are right.

The locations weren't right for ad tech collection, either. Boxes sat on the roofs of run-down motels in industrial neighborhoods, bolted to billboards above the freeway. They lined America's highways — drive far enough and the system would clock you. No single box was worth much. The value was in the network.

In a bid to raise cash in late 2023, Wireless Guardian added new technology that required box owners to install LPR cameras. The system now collects biometric data: facial recognition, gait recognition, and temperature. It could allegedly spot the cold metal of a gun concealed at the hip.

Far Away

If the boxes once made Dumas feel safer, that comfort didn't survive as he transitioned from hustler to fraudster. As investor funds streamed in from new box purchasers and out to earlier ones — dressed as data revenue — Dumas put as much distance between himself and his network as American geography allows.

Dumas decamped to Lahaina, Hawaii, shortly before fire rolled down from the hills and devoured the former whaling town. Front Street is rubble and construction fencing. The banyan tree — planted in 1873 — survived and stands in an empty lot. Dumas's mansion, purchased with diverted investor funds and perched safely above the town, survived the blaze. He stayed. There was no Lahaina anymore: just 115 crosses along Honoapiilani Highway and acre upon acre of scorched earth.

Wireless Guardian began to crack. The Intel relationship had soured, with the tech giant telling WG it would under no circumstances announce a partnership. Labyrinth was losing patience. By April 2024, the founders had elevated CTO Jimmy Cunningham — a 20-year veteran of the counterterrorism and counterintelligence apparatus — to CEO.

Vanished

Dumas told his girlfriend he was going fishing.

Each Wireless Guardian Pattern of Life box, operating at a gas station or convenience store, assembled a composite record for every person who came within range:
• RF layer: IMSI (the unique identifier of your SIM card, extracted without your knowledge or consent, the same data that requires a warrant when law enforcement collects it); MAC address; AAID; IDFA.
• Vehicle layer: License plate, vehicle make, model, and color from the LPR camera. Cross-referenced with the RF layer to link a device identifier to a vehicle.
• Biometric layer: Facial geometry from the PTZ camera, with autonomous tracking across 300 preset positions.
• Weapon flag: Thermal detection of body-carried concealed firearms via heat contrast. Not through vehicle bodies — physics prohibits it — but on any person within the camera range.
Each of these records is timestamped and GPS-tagged, linked to the same device identifier, and uploaded to a FedRAMP-authorized cloud with law enforcement access. The composite record is not an advertising profile. It is an intelligence dossier.

At 7 a.m. he backed a 25-foot boat out of Mala Wharf — a crumbling pier jutting from the charred remains of Lahaina — and pointed the bow west toward the Kealaikahiki Channel, the path ancient Hawaiian navigators took when they were leaving for good.

His girlfriend called the Coast Guard at 6 p.m.

The cutter Oliver Berry found the vessel the following morning, west of Lanai, rocking in open water. Empty. The search that followed covered 3,000 square nautical miles and drew more than 100 personnel from the Coast Guard, the Navy, and the Air National Guard — the precise constellation of federal agencies Dumas had spent a career courting in conference rooms from Atlanta to Washington.

They found nothing.

The Reckoning

Back on the mainland, acting CEO Cunningham took stock of the wreckage and decided to come clean. Two days after Dumas left the dock on June 10, 2024, Cunningham drafted a confession letter to box owners, describing his discovery of what the company was as "uncomfortable, painful, not fun." The board issued its own confession.

The Intel contract existed. It just ran backward. Wireless Guardian was buying software from Intel, not selling data to it. Intel was a vendor. The relationship investors had been shown — Intel purchasing data at $0.015 per device — was a screenshot, cropped and framed to conceal what the full document said. After months of requests, investors received that document two days before the scheme collapsed.

The revenue-sharing payments had been other investors' money. New equipment sales funded the distributions that made the data story credible, attracting new investors, who bought new equipment. The board, investors were told, had elected to warehouse the data for future use. Xanthon hadn't been paid and had cut the servers that processed the data pouring from the boxes. Those boxes stayed on their rooftops, cameras spinning, clocking license plates and heat signatures with nowhere to send the data. The Fourth Amendment end-run, dressed as a passive income opportunity, had run out of road.

Cunningham filed a RICO suit against his former colleagues. Labyrinth's supplier sued them for a million dollars in thumb drives. Between Dumas and the 200 investors sat a tier of resellers — bagmen, effectively — some of them victims themselves, some of them driving to Georgia weekly to go hunting with the CFO and discuss strategy. They sued.

A group of 200 box owners at the bottom — a Hampton Inn, a Lovers adult store whose clientele had particular reasons to expect their visits would go unrecorded, and a couple named Peter and Melissa, to name a few — got together and sued Intel in Cook County, IL.

Second Life

Nine months after Dumas left the dock, the owners of the 994 installed boxes received an email through the original Wireless Guardian infrastructure — same servers, same list. Someone still had the keys.

PatternView. The CEO is Jeff Hutchins, one of the plaintiffs in the Cook County fraud suit against Intel over the same boxes. He lost nearly $10 million on the network. He came back anyway.

Hutchins found a partner in The Digital Decision, a Virginia public safety consultancy whose founder, Robert LeGrande, served as Chief Technology Officer of the District of Columbia and testified before the Senate. The Digital Decision holds a GSA Schedule 70 federal contract. It markets facial recognition, wireless threat monitoring, weapons detection, and signals intelligence to local and federal government through a purpose-built procurement channel. LeGrande bought into the boxes, too, according to the Cook County complaint, losing money with everyone else. He looked at the wreckage and decided the technology was fine. The problem was the company.

PatternView sits in The Digital Decision's partner stack now, between a facial recognition firm and a wireless threat monitor, described in the clean language of the vendor catalogue: *accurate, reliable location data for decisions made with confidence.*

What Dumas built in the key of fraud — passive income, rooftop antennas, the data economy made accessible to ordinary Americans who would never see a dollar from it — LeGrande and Hutchins are finishing in the key to public safety procurement. Different key. Same song.

The Data

Dumas built a machine to find anyone, moved thousands of miles from it, and vanished into 64 million square miles of ocean. He left his surveillance system running.

The antennas lining America's arteries still orient toward the traffic below. The cellular backhaul is still uploaded. The data flows.

We noticed this network of boxes because the founder vanished and the money ran out. Ten thousand other boxes, on ten thousand other rooftops, belong to companies that will never make the news — because their founders didn't disappear, because their investors didn't sue, because their privacy pages are finished.

The air is full of us. It always has been. We just didn't know anyone was listening.

Lael Henterly, CLI, *founded Integra Intelligence, a boutique Seattle private investigation agency, in 2016. As a complex litigation investigator, she uncovers witnesses who substantiate white-collar crime allegations against corporate executives and public companies, specializing in securities fraud, antitrust violations, corruption, and qui tam matters.*
Henterly teaches civil litigation investigation at the University of Washington, where she also earned her journalism degree. She worked as an investigative journalist before transitioning to investigations. In 2025, she received the Anthony Golec Editor/ Publisher Award from TLI. She can be reached at lael@integraintel.com

