Flock Safety and FlockNova: A Complete Guide

From zero to expert on the cameras, the AI, the map, the alerts, and the data-fusion engine behind them

Joshua Michael
Email: josh@nexanet.ai

September 2, 2026

Contents

How to read this guide

This document is meant to take a reader with no background at all and leave them an expert on how Flock Safety's system works; the physical cameras, the artificial intelligence inside them, what they record, what a user can search for, and how the companion investigation product, **FlockNova**, turns an ordinary detail about a person into a full dossier and a movement history.

Because Flock is a surveillance company that makes strong public claims about what it does and does not do, this guide is careful to separate three different kinds of statements. Keeping them apart is what makes the rest of the document trustworthy:

- **What Flock says.** Marketing pages, product brochures, help articles, and public statements. Useful, but it is the company describing itself.
- **What the evidence shows.** Things visible directly in Flock's own software: the code that runs in its apps and browsers, its patents, its price lists, and a production data export. When this guide says "the code shows," it means code pulled from Flock Safety during my cybersecurity research, in the actual apps, not advertisements.
- **What it means.** Interpretation: reasonable conclusions drawn from the first two, clearly flagged as analysis rather than fact.

Part 1: The one-page version

Flock Safety is usually described as a "license plate reader company," but that is a marketing-engineered scope. In the title of its own patent, the company is described more accurately as a "dynamic surveillance network" (U.S. Patent 11,416,545 B1).

What Flock actually operates is a nationwide, connected **surveillance and investigation platform** with three layers that feed into each other:

1. **Sensors.** Cameras and microphones on poles, buildings, trailers, and drones that watch roads and public spaces and turn what they see into archivable, searchable records that can be retained on paid tiers of 30 days, one year, three years, or five years, subject to state law. These are not only plate readers. They photograph and classify vehicles, people, and objects, and some listen for gunshots.

2. **FlockOS.** A live map that gathers every camera, vehicle/person alert, incident, patrol car, drone, and 911 call into "one map" for a police department or a private security team, so an operator can watch and respond in real time.
3. **FlockNova.** A separate investigation tool that takes a single clue about a person (a name, a phone number, an email address, a license plate, even a mobile advertising ID from an app on their phone) and searches across public records, agency databases, breach/"dark" data, and phone-location data to build out everything connected to them, then draws it as a map, a timeline, and a relationship graph.

Flock's own phrase for how these fit together is **"Search Once. See Everything."**

Part 2: What Flock Safety is

The company. Flock Safety is the operating name of **Flock Group Inc.**, founded in Atlanta in 2017 by Garrett Langley and others. It began by selling automatic license plate reader (ALPR) cameras to neighborhoods and homeowners' associations, then expanded aggressively into policing, retail, and business security. It is one of the fastest-growing surveillance vendors in the United States.

The scale. Flock's own public materials describe a national network reading **more than 20 billion vehicles per month across 49 states**. It helps to hold that number against the size of the country's entire vehicle fleet: the United States has only about **297 million registered vehicles** in total (Federal Highway Administration, Highway Statistics 2024). Twenty billion reads a month is therefore not twenty billion different cars; it is the equivalent of scanning the nation's entire fleet dozens of times over, every month. In plain terms, the same ordinary vehicles are being photographed again and again, and that repetition is exactly what converts scattered sightings into continuous movement records. My own research into Flock's systems documented an operating sprawl of roughly **5,000 police departments, 6,000 private communities, and 1,000 businesses**, and a monthly read volume likely above 30 billion, including people. A production data export obtained from Flock's mapping systems in December 2025 contained **335,701 device and deployment records**, of which about 214,000 were marked in-service, about 83,000 were marked as *planned* (coverage intended but not yet installed), and about 38,000 were decommissioned.

This is one shared platform, not thousands of separate city systems. A town that buys Flock is not buying an island. It is joining a common network with shared software, shared map infrastructure, shared credentials, and, crucially, the ability to search and share across other agencies. A single vehicle read in one town can be visible, searchable, or shareable nationwide.

It is not only the police. People picture Flock as a police tool, but its own software enumerates several classes of customer: law enforcement, **homeowners' associations**, **property management**, **businesses**, **education**, channel partners, and demo accounts. That matters for privacy in two ways. First, a private HOA or business can be running plate readers on the roads around your home or workplace, then choosing to share that data with police. Second, on residential and business deployments the system logs the people who belong there: its access-logging fields classify a vehicle's occupant as **resident, employee, vendor, or other**, and support an "authorized access list" of permitted plates. In other words, an HOA's Flock system can quietly build a record of which cars (residents', workers', visitors', delivery drivers') come and go, and when. The same technology pointed at "outsiders" is also pointed at the community that installed it. There has notably been an opt-out/whitelist group that I attempted to register on but was denied.

Why "the camera is only the sensor." The single most important idea in understanding Flock is that the camera is the least interesting part. A camera by itself just takes pictures. The reach of the system comes from what happens *after* the picture: the search modes that let you query it, the alerts that fire off it, the sharing that spreads it between agencies, the exports that copy it out, and with Nova the fusion that ties it to a named human being. Keep that in mind as we go through the hardware, because the hardware is the on-ramp, not the destination. Every device is like a prison watch tower, constantly watching whether you have done anything "wrong" or not.

Part 3: The cameras and sensors

Flock does not sell a single camera. It sells a family of devices.

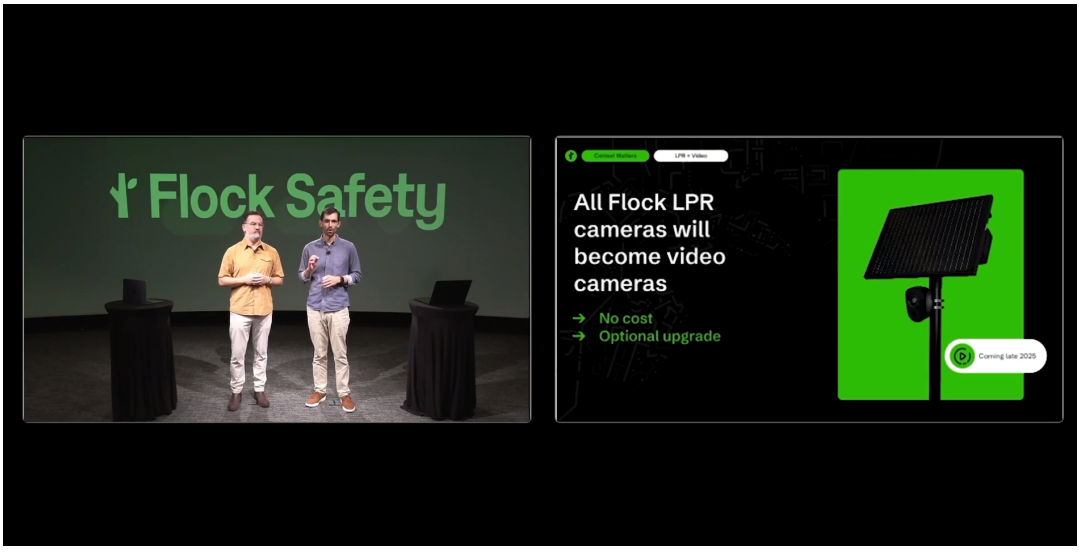
3.1 License plate readers: the “Falcon” family

The core product line is **Falcon**, with variants:

- **Falcon:** the standard fixed license plate reader. Solar-powered, cellular-connected, mounted on a pole beside a road. It photographs every vehicle that passes.
- **Falcon Flex:** a relocatable, battery-powered version that can be moved between locations.
- **Falcon Highway:** a version built for high-speed, multi-lane roadways.

A critical and widely misunderstood point: **a Flock LPR is not just reading plates.** Every Falcon is a camera that captures everything in its lens and its surroundings. The plate is merely the one object in that frame the company chose to market. The vehicle’s image, the people in and around it, their visible characteristics, and the timestamped location are all captured too. When you hear “license plate reader,” picture a camera that also records what the car looks like, what the person inside might look like, which direction it was going, and exactly when and where, because that is what it is.

Flock has made this explicit. At a company event it announced that **all Flock license plate readers will become video cameras** as a no-cost optional upgrade, collapsing any remaining line between “plate reader” and “surveillance camera.”



This matters because of what Flock tells the public about each product line separately. Its license-plate-reader FAQ, the version handed to communities and reprinted verbatim by police departments, states plainly that the cameras “do not use facial recognition technology and are not designed to identify drivers or passengers,” that they capture information “about vehicles, not people,” and that the system “does not collect personally identifiable information such as a driver’s name or address.” Its video-

camera product page markets the opposite capability: those cameras ship with AI analytics that Flock lists as **Guardian Mode, People Detection Alerts, and Visual Alerts** for "24/7 security coverage," alongside FreeForm, and it describes Guardian Mode as automatically detecting and tracking **people** and vehicles around the clock. So the reassuring "we don't do people" language is attached to the plate-reader line, while the people-detecting analytics live on the video line. The announcement that *every* plate reader becomes a video camera is what quietly erases that separation: the very devices sold to the public as "vehicles, not people" inherit the video line's people-detection features. Read together, the private capability release and the two public FAQs describe a large, quiet expansion of what the plate readers already mounted on the nation's roads are able to do, even as the plate-reader marketing keeps emphasizing their "limited" scope.

3.2 Video cameras: "Condor"

Condor is Flock's non-LPR video camera line, including pan-tilt-zoom (PTZ) models that can be steered and zoomed. Condor cameras provide general video surveillance and live-streaming rather than being dedicated plate readers, and they feed the same platform. The code also models Condor in several integration flavors (native Flock, IP-based, and so on), reflecting that Condor covers both Flock-made cameras and connections to other video.

3.3 Other device classes

Flock's device list also includes:

- **Sparrow** and **Owl.** Additional device classes in the product line (Sparrow is associated with compact/residential-style deployments; Owl appears as a device and streaming class).
- **Raven.** An **audio sensor**. Flock's own analytics fire an event literally named "Raven Audio Played," confirming that Raven captures audio that operators can listen to. In marketing, audio sensing is presented primarily as gunshot and alert detection, but the device records and plays back sound.
- **Picard.** An **edge-compute box**, including a PTZ variant. "Edge compute" means a small computer at the camera site that runs AI on the video *locally* before anything is sent to the cloud (more on this in Part 4).
- **Trailers.** Deployable camera trailers (including LPR trailers) that can be parked anywhere to create temporary coverage for events, investigations, or surges.

- **Talk-down and deterrence devices.** Speakers and related hardware that let an operator broadcast audio to a location ("talk down" to a person on camera).
- **Backhaul boxes.** Connectivity and networking hardware.
- **Wing gateways.** Devices that pull *other companies'* cameras into Flock. These get their own section (Part 7) because they dramatically expand what "a Flock camera" means.
- **Drones.** A full drone program (see 3.4).

3.4 Drones: the "Aerodome" drone-as-first-responder program

Flock's device list includes an entire drone ecosystem: drones themselves, batteries, camera payloads, controllers, controller boxes, docking stations, and drone radar. This is Flock's **Drone-as-First-Responder (DFR)** capability (built around its Aerodome acquisition): docked drones that can launch automatically in response to an alert or a 911 call, fly to a location, and stream live video back to the same map operators are already watching. In the investigation product, drone *flight logs* (every flight's path, altitude, and timing) can also be searched (see Part 13).

3.5 The honest summary of the hardware

Put together, a Flock deployment in a given area can include: fixed and relocatable plate readers, general video and PTZ cameras, audio sensors, edge AI boxes, portable trailers, talk-down speakers, gateways that absorb third-party cameras, and drones that launch on demand. Every one of these is a node that produces searchable records and can trigger alerts. That is the collection layer. Everything in Parts 4 through 12 is about what the platform *does* with what these devices collect.

Part 4: The AI behind the cameras

The intelligence in a Flock deployment lives in two places, and knowing the difference matters.

4.1 Edge AI versus cloud AI

- **Edge AI** runs *on the camera* (or on a nearby Picard box). Evidence from a captured Flock edge-camera software snapshot shows on-device object-detection models: small neural networks (in the common SSD and YOLO families, packaged as

TensorFlow Lite files) tuned to run fast on limited hardware, with configurable confidence thresholds. This is what lets a camera decide, in real time, “that’s a vehicle,” “that’s a person,” “that’s a license plate,” without asking the cloud first.

- **Cloud AI** runs on Flock’s servers and handles the heavier lifting: the natural-language “FreeForm” search, large-scale matching, and the fusion work in Nova.

Practically: the camera does fast recognition locally, and the cloud does the deep search and cross-referencing.

It is also worth being precise about “always on.” A plate reader fires on each passing vehicle and stores discrete detection events; a video camera can record continuously; and the audio sensors keep only short event clips (Part 4.6). The network is always available to observe and classify. What each device *retains* differs by product.

A note on OCR. A plate read is a machine *proposal*, not a fact. Angle, glare, darkness, motion blur, mud, a novelty frame, or lookalike characters can change the answer, which is why the search tools support fuzzy and partial plates and why the vendor’s own policy says a computer’s plate read should be visually confirmed. Errors here are not academic; they are how the wrong person gets stopped (see Part 10).

4.2 Vehicle Fingerprint: how a car becomes a searchable identity

Beyond reading plates, Flock’s headline computer-vision feature is what it markets as **Vehicle Fingerprint** (or “vehicle signature”). Instead of matching only on a plate, the system builds a description of the vehicle itself. Flock’s own code contains the structure of this fingerprint, and its fields include:

- **Make** (manufacturer),
- **Body / type** (sedan, pickup, SUV, van, and so on),
- **Color** (stored precisely, down to a color hex value),
- **Build/model options**, and
- **Identifiers**, meaning distinguishing visible features, each carried with a **confidence score**.

What this means in practice: even if a plate is dirty, missing, covered, or swapped, the vehicle can still be searched by *what it looks like*. Flock markets this as being able to find, for example, a specific color and body style of truck. The “identifiers” here are not vague: the captured attribute classes name them directly, and they include a vehicle’s **roof/top rack, back rack, bumper stickers, window stickers, and tool box**, alongside make, type, color, and the plate-visibility state. Those are exactly the details a human

witness would mention, now recorded and searchable per detection. In Flock's marketing and in its patent these appearance features are explicit; in the captured field structure they appear as scored attributes attached to each sighting.

There is a sharper edge here, and it undercuts the obvious evasion. The plate-visibility field is itself one of the stored, searchable states, with values the code spells out as `plate`, `unknown`, `no_plate`, and `plate_cover`. So "no visible plate" is not an absence of data; it is a filterable attribute in its own right. The fingerprint also includes a `vehicle_vector`, a numeric appearance embedding, which lets a vehicle be matched to earlier sightings by how it looks even when there is no plate text at all. Covering, removing, or swapping a plate does not take the car out of the system; it only moves the search from the plate to the body.

4.3 FreeForm: searching by plain-English description

FreeForm is Flock's natural-language search, and it is the feature that best captures how far past "plate reader" the system has gone. Instead of typing a plate, you type a description in ordinary words, and the system finds matching people or vehicles in the video. Flock's own product examples are exactly the kind of thing a witness would say:

- *"man in blue shirt and cowboy hat"*
- *"dark SUV with rear bumper damage"*
- a landscaping or work truck by its look rather than its plate

The diagram below shows why that works: a single camera frame is pulled apart by the AI into searchable vehicle and person attributes, so an ordinary phrase resolves to a specific time and place.

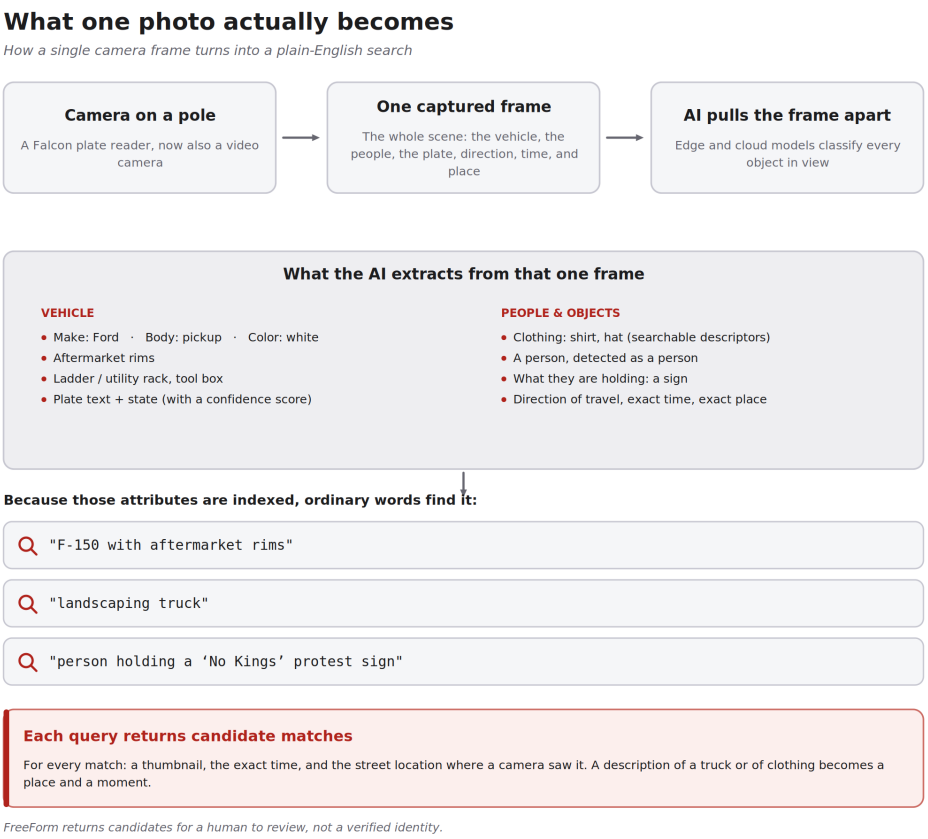
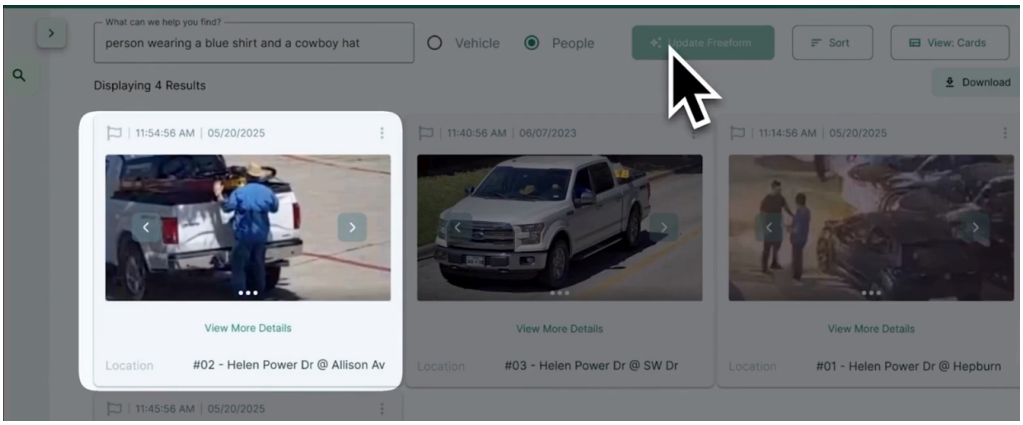
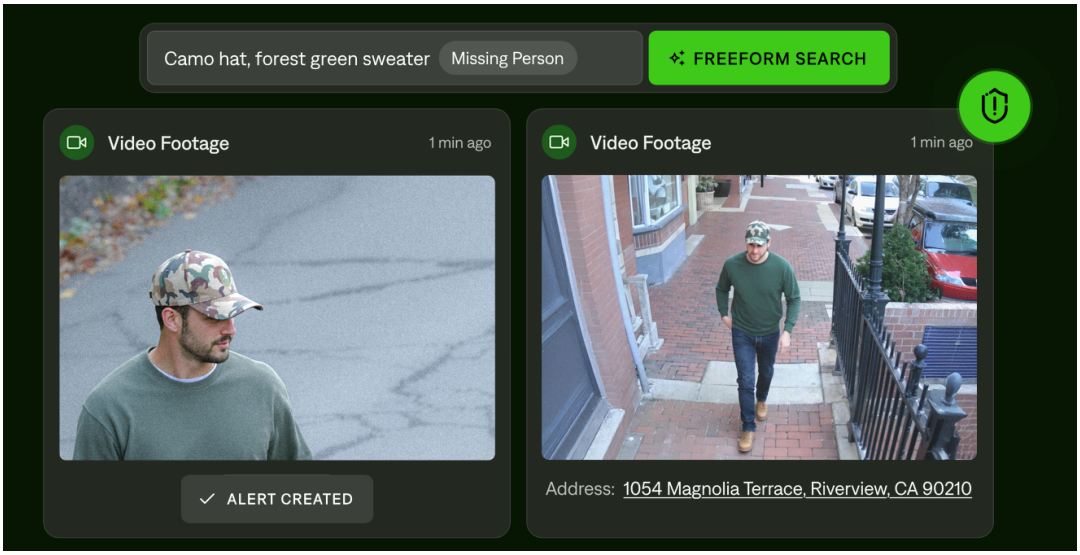


Diagram: author's illustration, based on Flock's FreeForm product and US Patent 11,416,545 B1.

The screenshot below is Flock's own FreeForm interface. An investigator typed *"person wearing a blue shirt and a cowboy hat,"* flipped the toggle from **Vehicle** to **People**, and the system returned candidate people from video across the camera network, each with a time and a location.



A second Flock demo shows what happens next: a description like *"camo hat, forest green sweater"* tagged **Missing Person** returns matching video, attaches the **street address** where the person was seen, and offers to create a standing **alert** for future matches. Description in, location and a watch order out.



Flock draws a careful public line around FreeForm's people search, and it deserves to be stated exactly as Flock states it and then next to what the code shows:

- **What Flock says:** FreeForm people search uses only *observable, non-biometric* characteristics like clothing and visible accessories, is "not designed to identify a specific person," uses **no facial recognition or biometrics**, and runs **only on enabled video cameras, not on license plate readers**.
- **What the code shows:** FreeForm is real and backend-powered. Behind that plain text box sits real structure: separate `VEHICLE` and `PEOPLE` search classes, versioned search endpoints, fields for the query text, date range, reason, offense type, and case number, targeting of both your own and shared cameras, and result paging. There is also a content-moderation layer that classifies each prompt and can **warn, block, or allow** it and, notably, when it meets a value it does not recognize, it **defaults to "allow."**

A crucial honesty point that Flock itself makes: a clothing match is not an identity. Many uninvolved people can satisfy "blue shirt and cowboy hat," and clothing changes by the hour. FreeForm returns *candidates for a human to review*, not a verified person.

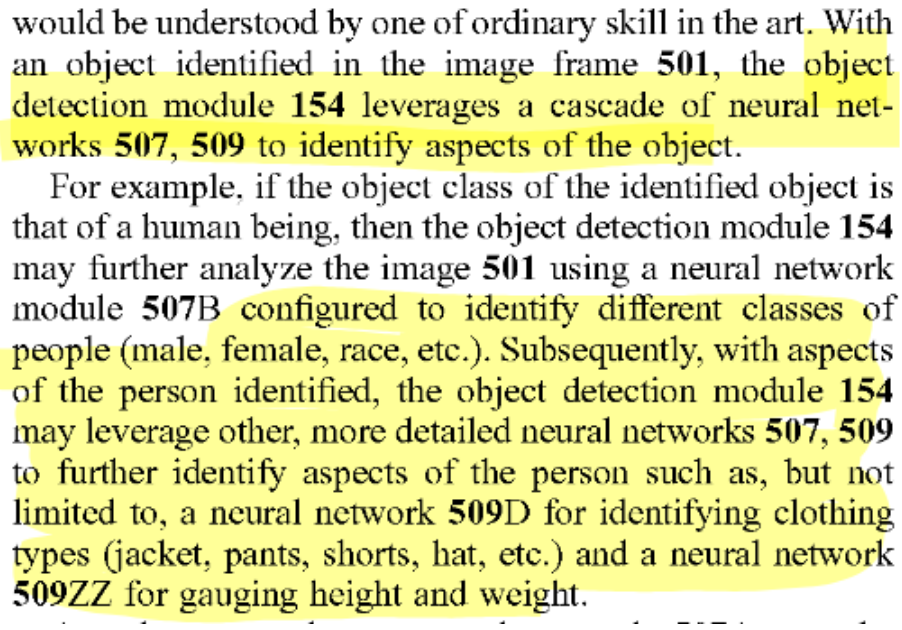
4.4 People detection and alerts

Separately from FreeForm, Flock supports **person detection** as an alertable event. Its code models person-detection filters and alerts with tunable minimum confidence, day-of-week and time-of-day windows, specific cameras/networks, and a policy. In other words, an operator can set the system to watch a location and notify them when the AI detects *a person* (matching configured parameters) at a chosen place and time.

4.5 How the AI classifies *people*, and the facial-recognition question

FreeForm searches people by clothing. But Flock's patent describes an AI that goes considerably further in analyzing people, and this is worth reading closely because it is the company describing its own invention to the patent office.

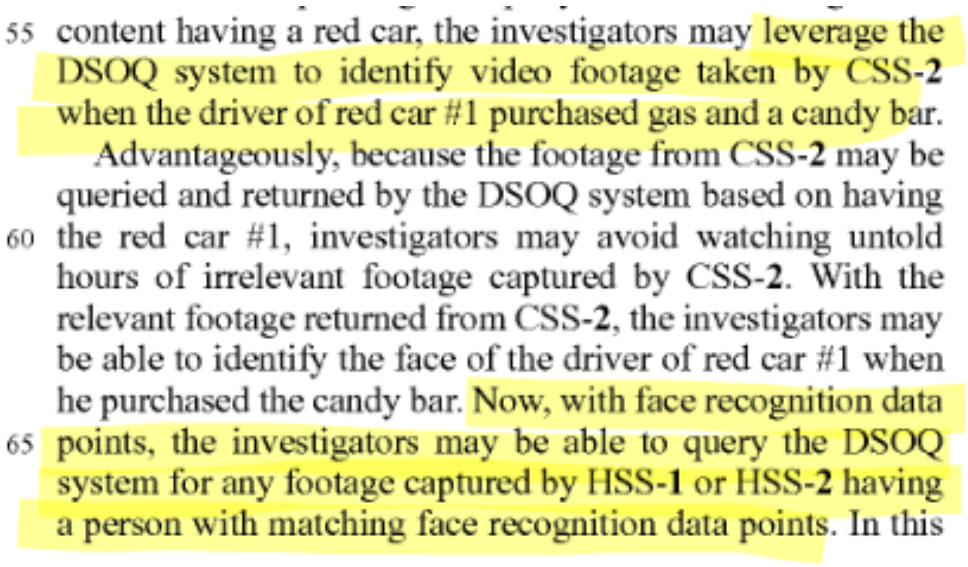
The patent says that when the object-detection module decides an object is a human being, it runs "a cascade of neural networks" to pull the person apart attribute by attribute. In the patent's own words, it can analyze the image to identify **"different classes of people (male, female, race, etc.)"**, then use more detailed networks to identify **clothing types (jacket, pants, shorts, hat)** and a dedicated network **"for gauging height and weight."**



would be understood by one of ordinary skill in the art. With an object identified in the image frame **501**, the object detection module **154** leverages a cascade of neural networks **507**, **509** to identify aspects of the object.

For example, if the object class of the identified object is that of a human being, then the object detection module **154** may further analyze the image **501** using a neural network module **507**B configured to identify different classes of people (male, female, race, etc.). Subsequently, with aspects of the person identified, the object detection module **154** may leverage other, more detailed neural networks **507**, **509** to further identify aspects of the person such as, but not limited to, a neural network **509**D for identifying clothing types (jacket, pants, shorts, hat, etc.) and a neural network **509**ZZ for gauging height and weight.

The same patent goes on to describe **"face recognition data points,"** the ability to query the surveillance network for any footage containing a person whose facial feature data matches, in order to find that person across unrelated cameras and reconstruct a timeline of where they went.



content having a red car, the investigators may leverage the DSOQ system to identify video footage taken by CSS-**2** when the driver of red car #1 purchased gas and a candy bar.

Advantageously, because the footage from CSS-**2** may be queried and returned by the DSOQ system based on having the red car #1, investigators may avoid watching untold hours of irrelevant footage captured by CSS-**2**. With the relevant footage returned from CSS-**2**, the investigators may be able to identify the face of the driver of red car #1 when he purchased the candy bar. Now, with face recognition data points, the investigators may be able to query the DSOQ system for any footage captured by HSS-**1** or HSS-**2** having a person with matching face recognition data points. In this

So the honest answer to “does Flock do facial recognition and profile people by race, sex, and body size?” requires holding three true statements side by side and refusing to collapse them into one:

1. **Flock publicly denies using facial recognition or biometrics today.** It says its systems are vehicle-focused and that FreeForm people search is explicitly non-biometric.
2. **Flock’s patent describes exactly that capability:** race and sex classification, height and weight estimation, clothing analysis, and face-recognition data points used to track a person across cameras and build a movement timeline.
3. **The captured, currently-examined software does not show a deployed facial-recognition feature running.** There was no live face-matching function in the code that was inspected.

The precise conclusion: **Flock patented a system that includes facial recognition and race/sex/height/weight profiling of people, currently says it does not use facial recognition, and the examined software does not show it deployed.** A patent is what a company reserved the right to build, not proof of what it runs today, and a current marketing denial does not erase what the patent contains. All three statements are true at once, and anyone who quotes only one of them is misleading you. (It is also worth remembering that even without any face matching, Flock’s FlockNova app integrates with FlockOS and lets an investigator search agency records by race, sex, height, weight, hair, eyes, build, and scars/marks/tattoos; see Part 13.)

4.6 Audio detection (Raven)

Flock markets audio detection for gunfire, fireworks, street takeovers, and vehicle collisions. In the app's own alert code these arrive as classifications like **"Single Gunshot"** and **"Multiple Gunshots,"** tied to the Raven audio sensor and dropped onto the map as an alert with a time and a location, which can then trigger a search for nearby plates, video, or units.

The important distinction is between *continuously listening for an event* and *continuously recording intelligible speech*. Flock's current explanation says the sensor evaluates roughly five-second windows locally, keeps only the clips tied to a qualifying event, and does not recognize speech or conversations. That is the vendor's representation, not an independent audit; verifying the exact firmware, model, and storage behavior would take testing the device itself. Treat audio detection as a real, marketed capability of the audio layer whose accuracy this evidence cannot vouch for.

Part 5: What the cameras actually capture

Pulling Parts 3 and 4 together, here is the concrete list of what a Flock deployment records, based on the device list, the edge models, and the data structures in the code:

- **License plate text and state**, including exact, fuzzy, and partial-plate handling.
- **Vehicle characteristics:** make, model/build, color (to a hex value), body type, and scored visual identifiers, all with confidence values (the Vehicle Fingerprint).
- **People and objects as classes.** The camera's own AI label set includes `person`, `vehicle`, `car`, `truck`, `bus`, `motorcycle`, `bicycle`, `license plate`, `trailer`, and even `cat` / `dog` / `pet`. This confirms the cameras detect and categorize *people and objects*, not only plates. (This is detection and classification. It is not, in the examined code, identification of a named individual.)
- **Direction, time, and precise location** for each detection.
- **Clothing and visible accessories,** as searchable descriptors through FreeForm's people search (per Flock, non-biometric).
- **Audio,** through Raven sensors and through 911 integration, including live and recorded sound that operators can play back.
- **Live video:** Condor and other video cameras can be streamed live (see GoLive, Part 8).

So when a Flock camera “sees” you drive by, the record is not “a plate number.” It is potentially: the plate, a description of your vehicle with a confidence score, the direction you were traveling, the exact time, the exact camera location, and a stored image, all of it searchable later, and all of it able to trigger an alert in real time.

Part 6: What can actually be searched

Flock’s search web app registers a fixed set of search *modes*. These are visible directly in its production code as distinct routes, which makes them solid evidence of what the platform is built to do:

1. **Plate lookup** (`/lookup`): search by a full or partial plate, with exact, fuzzy, and even *excluded* plates, across chosen time ranges and chosen cameras/networks. A mandatory “reason” field accompanies the search.
2. **Visual search** (`/visualSearch`): search by a detected object or vehicle rather than a typed plate.
3. **General search** (`/search`): the standard search session, carrying vehicle-description fields, case/offense/reason metadata, time, and camera scope.
4. **Multi-Geo search** (`/multiGeoSearch`): a *place-and-time intersection* search. An investigator picks several camera-plus-time selections and asks which vehicles appear across all of them, **without needing a plate to start**. This is how you go from “who was near here at this time, and also near there at that time” to a candidate list. (It is not a continuous GPS track and it is not phone geofencing; it is an intersection of discrete camera sightings.)
5. **Convoy search** (`/convoy`): takes one vehicle or detection and finds vehicles that appear to be **traveling with it** (co-travel analysis), to reveal companions, escorts, or a group moving together.
6. **People search** (`/peopleSearch`): the people-oriented search surface.

On top of those, Flock’s mobile app supports a **run-plate** flow: an officer points a phone camera at a plate, the phone’s on-device model reads the characters, and it checks them against hotlists and history, turning any phone into a plate reader.

Partial-plate searching deserves a specific note: the system explicitly handles incomplete plates and even checks for the classic "O versus 0" ambiguity. You do not need the whole plate to search. (There is a real guardrail here worth crediting: partial-plate and no-plate searches are capped to windows of 30 days or less in the captured client.)

Flock also markets a set of higher-order analyses that derive *relationships* rather than look up a single vehicle:

- **Plate-swap** flags when a plate and vehicle appear mismatched, hinting at a swapped or covered plate.
- **Convoy / co-travel** looks for vehicles repeatedly seen near a target vehicle.
- **Hotspot** looks for concentrations of activity by place or time.

Each of these is an *inference*. Two cars seen together repeatedly might be coordinating or they might just be neighbors, commuters, a delivery route, a shift change, or two vehicles funneled onto the same road by the map. A responsible use of any of these keeps the underlying observations, the time window, and the plausible innocent explanations attached to the result, because the machine is proposing a pattern, not proving intent.

The takeaway: you can search Flock by a full plate, a partial plate, an excluded plate, a vehicle's appearance, a plain-English description, a person, a place-and-time intersection, a travel companion, a sign you are holding, or a behavioral pattern. That is a far wider set of capabilities than "look up this plate."

Part 7: Wing Gateways and the Business Network

This is one of the most important and least-understood parts of the system, so it gets its own section.

Wing Gateway is a Flock device family whose job is to **pull cameras that Flock did not make into Flock's platform.** Flock's own integration list names the third-party video systems it connects to, including major names in the industry (Avigilon, Genetec, Milestone, i-PRO, Uniview), as well as pole and streetlight camera integrations (Ubicquia) and a "custom" catch-all. A Wing gateway sits on a network, speaks to those existing cameras, and makes their feeds available inside Flock.

The consequence is the single most important thing to understand about Flock's true footprint:

> **A "Flock camera" does not have to be a Flock camera.** A private business's existing security cameras, a school's camera system, a parking garage's system, an apartment complex's cameras, or a city's traffic cameras can be brought into Flock's search and live-view plane through a gateway and a sharing agreement.

The mechanism that makes those third-party (and other agencies') cameras usable by someone else is Flock's **sharing** system. Flock's code defines fine-grained, feature-by-feature sharing permissions, so one organization can grant another specific rights to its cameras: the right to **search** them, to see them on a **hotlist**, to view them **live** (GoLive), to view **historical** video, to **download** video, to change **imaging settings**, to operate **PTZ** controls, and to use **advanced analytics**. This is how one entity's cameras become another's investigative tools.

Flock separately markets a **Business Network** that places participating private businesses' cameras within law-enforcement search scope. Between gateways and business networking, the searchable camera universe extends well past the poles that carry Flock's own branding, and it can span neighborhoods, private commercial property, and public agencies within the same area.

Worth knowing too: some third-party cameras brought in through a gateway are not just video. Flock's own device list marks Wing (and the Ubicquia streetlight variant) as **plate-reading capable**, so an ordinary business camera can become a license plate reader once it joins the network. And the connections run in the other direction as well: Flock's integration list shows it also ingests from or ties into other large surveillance platforms, including **Axon** (police body cameras and evidence), **Genetec**, and **Fusus** (a real-time crime-center system that itself aggregates many camera feeds). The practical effect is that Flock is a hub that both absorbs other camera estates and plugs into the broader police-surveillance ecosystem. One detail inside the data model makes this concrete: each detection record carries a **source tag** marking who originally captured it,

and the code's values include `FLOCK`, `AXON`, and `GENETEC`. So a single search run inside Flock can return footage that an Axon or Genetec system, not a Flock camera, actually recorded of you.

Part 8: FlockOS, the "one map"

Everything in the sensor layer flows up into **FlockOS**, which Flock markets under the line **"One map. Smarter response."** FlockOS is the real-time operational picture: a single map where an operator sees cameras, detections, alerts, incidents, patrol units, drones, and 911 calls together, and responds.

8.1 It is built on a professional mapping stack

FlockOS is built on **Esri's ArcGIS**, the same industrial geographic-information system used across government and defense. This matters because ArcGIS is not just a way to draw dots on a map; it brings heavy geospatial analysis. Investigation into Flock's systems found that the credentials tied to this mapping layer carried premium ArcGIS capabilities including **routing, closest-facility analysis, service-area generation, origin-destination cost matrices, and vehicle routing**: the exact tools you would use to answer "which unit is closest," "what's the fastest route to intercept," and "what area can be reached in X minutes." In other words, the map is not passive; it can compute movement.

8.2 What lives on the map

FlockOS's common map assembles many layers into one view:

- **Camera and device layers:** every camera, sensor, trailer, and drone, with location, direction, status, and health.
- **Vehicle and person alerts:** plate hits, hotlist hits, and person-detection alerts, placed at the camera that saw them, with time, confidence, and media.
- **CAD and AVL:** computer-aided dispatch incidents and automatic vehicle location (live patrol-car positions), so dispatch and surveillance sit on the same map.
- **Raven audio events** and **drone telemetry** (with live states like docked, recording, streaming).
- **Flock911 events:** live 911 calls with location and audio (Part 9).
- **Custom agency layers:** an agency can add its own map data.

- **Heatmaps:** the map component explicitly supports heatmap rendering, so density of detections or events can be shown as intensity rather than individual points.
- **Regions of Interest (ROI) and geofences:** investigators can **draw polygons** on the map to define an area to watch or search. These drawn shapes are saved with the search. That means the system stores not just what you searched for but *exactly which streets, lanes, or perimeters* you were focused on, effectively recording stakeouts and monitored checkpoints.
- **Camera groups:** named, shareable sets of cameras, which double as a directory of where a given alert is broadcast.

8.3 Agencies pour their own data into the map

The “custom agency layers” bullet above is bigger than it sounds. Evidence, including code paths that fetch per-organization map layers, public examples, and a statement from a police-department GIS employee, indicates that participating agencies **share their own geographic data into Flock’s mapping plane** so FlockOS can render it. That can include patrol beats and zones, dispatch (CAD) zones, district boundaries, address and 911-address points (sometimes with subscriber names), planned camera deployments, and, in some cases, **building floor plans and site-security overlays**. The map an operator sees is therefore a fusion of Flock’s sensors *and* the agency’s own operational geography. And it runs both ways: when an investigator draws a search area, that geofence can be stored as a layer too, so the map also records *where investigators have been looking*, which is its own form of sensitive intelligence.

8.4 Live video: “GoLive”

FlockOS ties into live streaming. Its code shows a **GoLive** path: from a camera’s ID, the operator requests a live stream and receives a streaming URL and a viewer token, watching in near-real-time (with a heartbeat keeping the session alive and picture-in-picture support). The list of which cameras can be streamed is right there in the client. So the map is not only historical dots; it is a launch point into live eyes on a location.

Part 9: Flock911, Prepared911, and CAD/records integration

Flock connects to the emergency-response stack, and this pulls some of the most sensitive data of all onto the map.

- **Flock911 / Prepared911** brings **live and replayable 911 call audio and transcripts** into FlockOS. Flock's code for this is specific: a 911 alert record carries the **caller's phone number, an estimated latitude/longitude and address, live/recorded audio, and a transcript.** The operator's screen can even **compute the distance between the caller's estimated location and the responding officer's phone.** Audio can be played, paused, scrubbed, and replayed.
- **ForceMetrics** and **RMS** integrations connect records-management systems (the databases where police store reports, arrests, and case data) into the environment.

The plain reading: when Flock911 is in use, a 911 caller's number, location, address, and the audio of their call can appear on the same operational map as camera alerts and patrol cars, visible in a browser.

Part 10: Hotlists and alerts

A **hotlist** is a watchlist of plates. An **alert** is what fires when a camera sees something on a list (or matching a saved search). This is the day-to-day heartbeat of the system, and the code shows exactly how it works.

A hotlist is not a warrant, and nothing in the system requires one. Adding a plate to a hotlist is an administrative act, not a judicially authorized search. The entry fields for a case number and a reason exist, but as with the rest of the platform they are free-text and optional; the software does not verify that a case number is real, that a reason is legitimate, or that any legal process backs the entry. Who ends up on a hotlist, and why, is left to the discretion of the individual agency or, on a private deployment, the HOA or business running the cameras. In the examined software there are no visible controls that would stop an operator from placing an arbitrary, innocent person's plate on a list, for any reason or none, and there is no built-in review, mandatory expiration, or notice to the person listed. The only limits are whatever policy a given customer chooses to impose on itself.

How a plate becomes an alert. An organization creates a hotlist and adds plates to it, one at a time or in bulk by uploading a CSV file. Each hotlist entry stores far more than a plate number. Flock's hotlist code shows entries carrying: the **plate**, **state**, a **reason**, a **case number**, an **expiry**, free-text **notes**, and **registered-owner information** ("plate and owner info," described as law-enforcement-only owner data). When any camera in scope reads a plate on the list, a **hit** becomes an **alert**, delivered to the operator with the camera, location, time, and the enriched owner and case details attached, and dropped onto the FlockOS map.

Owner enrichment. This is worth stating plainly: a hotlist hit can arrive already decorated with the **registered owner's identity**, pulled from vehicle-registration/records sources. The alert is not just "this plate was seen." It can be "this plate, registered to this person, was seen here at this time."

Inter-agency notification. Flock's code reveals that when two different organizations put the *same* plate on their lists, the system emails both. Its own warning text reads that "an email notification, containing the plate number only, will be sent to you and any organization entering the same plate." So watchlists silently connect agencies watching the same vehicle.

Saved searches and vehicle/person alerts. Beyond plate hotlists, operators can save searches and create alerts on vehicle *descriptions* (Vehicle Fingerprint criteria) and on *person detection*, scoped by camera, network, days of the week, time of day, and confidence. Combined with drawn ROI polygons, this turns "watch this area for this kind of vehicle or a person, on these days, at these hours" into a standing, automated alert.

Volume tiers. The code even shows that certain organizations are flagged for very high alert limits (hundreds of simultaneous hits) while others are rate-limited, a hint at how much data the busiest customers are consuming.

A hit is not probable cause, and Flock's own software says so. This is one of the most important sentences in the whole system, and it comes from Flock's own interface: a captured hotlist screen states that **"custom hotlists alone should never be used as probable cause."** The vendor is admitting, in its own product, that a machine match is not a lawful basis to act. An alert is a reason to *look*, not a reason to *stop, search, or arrest*. When that line gets ignored, when an officer treats a beep on a screen as certainty, is when innocent people get pulled over at gunpoint over a misread plate.

How alerts go wrong, and why it lands on ordinary people. An alert is only as good as the match behind it, and the match can fail in ordinary, predictable ways:

- **OCR misreads:** a dirty, bent, or shadowed plate read as the wrong characters (the classic "0 versus O," "1 versus I," "8 versus B").
- **Cloned or stolen plates:** a criminal running your plate number on their car means *your* plate lights up the hotlist.
- **Borrowed, rented, and sold vehicles:** the car on the list is not driven by the person the list is about.
- **Stale entries:** a plate left on a hotlist after a case closed, still triggering stops months later.
- **Wrong-jurisdiction collisions:** the same plate string exists in another state.
- **Overbroad lists:** a bulk CSV upload that swept in plates it should not have.

None of these require anyone to "hack" anything. They are the normal failure modes of automated matching at scale, and every one of them can put a person who did nothing wrong into a police encounter.

Suppression. Operators can *suppress* hits, which quietly removes them from alerts. That is useful for cutting noise, but it is also a consequential, low-visibility policy lever: it decides who gets mobilized and who does not, and it can be used to hide as easily as to de-clutter.

Part 11: Retention and sharing

How long data is kept. Flock's public policy describes a **default retention of about 30 days** for standard footage, after which it says data is deleted on a rolling basis. But Flock's own price list includes paid **retention extensions of one year, three years, and five years** per camera. So the "30 days" figure is a default, not a ceiling; longer histories are a purchasable product. (Flock's current public evidence policy describes extended LPR retention only up to a year under conditions, which does not match the multi-year options in the captured catalog, and these tiers are offered subject to state law, which caps retention in some jurisdictions.)

Retention length is the difference between two very different capabilities. A 30-day window can reveal your current commute or a recent trip. A multi-year window supports seasonal baselines, “you always go here on Tuesdays,” household changes, and long-run co-travel analysis. **Repetition is what turns movement data into intelligence, and retention is what preserves the repetition.**

Also worth knowing: a 30-day deletion of raw footage does not necessarily reach everything derived from it. Exports, downloaded copies, investigation files, audit logs, search history, alerts, and anything already shared to another agency are separate artifacts with their own lifespans. Alerts in particular run on their own short clock: the map and alert layer carries a retention constant of about **seven days** (`ALERT_RETENTION_TIME`), a different window from the roughly 30-day image retention, so a notification object and the footage it points to can expire on separate schedules.

Sharing and national lookup. Flock’s sharing system (Part 7) lets organizations grant each other access, and its settings distinguish between being **discoverable** to others (within 50 miles, within a state, or **nationwide**) and **auto-accepting** shares (statewide or within a set radius). Being nationally *discoverable* is not the same as automatically sharing data with everyone, but it is the mechanism by which a local camera network becomes part of a national lookup fabric. Flock markets national cross-agency search across connected records, LPR, jail, and public-records data.

Part 12: The patent, a “dynamic surveillance network”

Flock holds U.S. Patent **11,416,545 B1**, “System and method for object-based query of video content captured by a dynamic surveillance network” (assigned to Flock Group Inc.; inventors Garrett Langley and Matt Feury; granted August 2022). It is the clearest statement of the company’s own vision, in its own words to the patent office.

The **issued claims** describe a system that:

- captures video and tags each object with **time, location, and object class/aspect** data;
- lets a user search that object-indexed video database;
- returns matches **linked to playable video**, with **confidence scores**;
- explicitly draws from **neighborhood, commercial, traffic, and portable** camera sources, that is, stitching together otherwise-unrelated cameras into one searchable network; and

- can raise an **alarm** when a matching object is detected.

The **specification** (the broader description, wider than the enforceable claims) goes further. It describes classifying **humans, vehicles, bicycles, and animals**; person classes including **sex, race, clothing type, and estimated height and weight**; **object fingerprints**; historical similarity comparison across cameras; **face-recognition datapoints** to find a person across sources and build a timeline; and reports that include a **map, a timeline, and "out of place" analysis.**

The honest crosswalk (as in Part 4.5): object-indexed video search, shared-source networks, playable results, match alarms, and vehicle/person appearance attributes *are* reflected in the shipping products. The face-recognition datapoints and the race/sex/height/weight classifiers are **in the patent but not found in the examined software, and are publicly denied.** The patent tells you what Flock designed the system to be capable of. It does not tell you what is switched on.

Part 13: FlockNova, in full

Everything above is the collection and response side. **FlockNova** is the investigation side, and it is where a license-plate network becomes something much larger. This is the part most people have never heard of, and it is the part that matters most for personal privacy.

13.1 What FlockNova is

FlockNova (also written "FlockNova" or just "Nova") is a browser-based **investigative data-fusion tool**. Its own application title is "FlockNova Law Enforcement Investigations." Functionally, it is a search engine for people: you give it one identifier or one location, and it fans a single query out across many databases, merges everything it finds into one workspace, and shows it to you as a browsable list, a map, a timeline, and a relationship graph.

Flock markets it with the phrase **"Search Once. See Everything,"** and public reporting has quoted Flock's ambition for the tool in even broader terms; the company has spoken of a goal to "eliminate all crime." Whatever one makes of that ambition, the design goal is clear from the code: **a single selector is treated as a starting point for many record systems at once.**

13.2 Where it came from

Nova is not something Flock built from scratch. The evidence shows it is a rebuild of a tool called **Lucidus**, a startup Flock acquired in early 2025. Flock's own marketing text says outright, "Lucidus Tech is now Nova by Flock Safety," and older parts of the code still carry Lucidus branding and legal language (one leftover legal notice even says client data is stored in a "Lucidus Technologies information system"). Two other names appear in the code lineage, **CodeFour** (a partner or branded deployment) and **Healthcare Safely** (an older related domain), though the evidence supports a partnership or shared-code relationship rather than confirming acquisitions.

Why the origin matters: Nova's DNA is a **data-broker / OSINT (open-source intelligence) aggregation tool**, wired into Flock's camera network. That combination, a people-search aggregator plus a nationwide sensor grid, is the whole story.

13.3 The warrant and case-number reality

This is the point most worth understanding, and the evidence is unusually clear.

Nova does not, in its own front-end logic, require a warrant, a case number, or a stated purpose to run most searches.

Here is what the code shows:

- A **case number is optional and cosmetic** in the ordinary search path. It is a value typed into a box and stored in the browser; the routine that actually runs a search does not require it or even read it. Most searches (ordinary, advanced, linked, and bulk) can be started without transmitting any case number, purpose, or record of legal authority. (A backend server *might* independently reject a search, but that cannot be seen from the front-end, and there is no visible sign of it.)
- The **case-number prompt is easy to bypass.** It only appears if a specific per-user flag is set, and even when it appears, in one version it can simply be closed, and in another it becomes dismissible as soon as you type any character. When submitted, the case number is sent with **no validation**: no check that it is real, active, assigned to you, or connected to an actual investigation.
- An **"investigation ID"** that looks official is just an identifier **generated in your browser** before you open a new investigation. It corresponds to no verified legal matter.

- Even the integrated LPR form that labels a section **“Justification (Required)”** does not actually enforce it: the validation only checks that you entered a plate or an area. Leave the reason blank and it quietly defaults to the words **“Nova Investigation.”**
- Several sensitive actions have **no audit trail written next to them** at all, and the audit logging that does exist is “fail-open” (if logging errors out, the search proceeds anyway).

The plain-English version: **the accountability controls in Nova are largely honor-system prompts, not enforced gates.** A case number in Nova is an internal label. It is not a warrant, not a judge’s approval, and not proof that a search was lawful. The front-end provides no reliable way to tell a properly authorized search from an unauthorized one: a search with a fabricated case number and a search backed by a real warrant look identical to the system.

(An important fairness note that the evidence itself insists on: these are findings about the *front-end*. It remains possible that Flock’s servers enforce checks that cannot be seen from the outside. But the misleading, easily-bypassed accountability signals in the client are real regardless.)

13.4 Every way Nova can search for a person

Before the list, one clarification, because Flock’s system has **three different things people lump together as “AI search”** and they are not the same:

- **FreeForm** (Part 4.3) searches *video* for a person or vehicle by plain-English *appearance* (“blue shirt and cowboy hat”).
- **Nova’s quick-search predictor** (this section) takes a typed *identifier* (a name, email, plate, SSN) and routes it to the right databases.
- **Ava** (Part 13.10) is a chat assistant that reads a request and can *run searches for you.*

The first searches how someone looked. The second follows a piece of data. The third lets a model decide what to look up. Keeping them apart is what stops the conversation from becoming confused.

When you type into Nova’s search box, the quick-search predictor looks at what you entered and guesses what kind of identifier it is, using pattern-matching. It recognizes and can search on:

- **Name**
- **Email address**
- **Phone number**

- **Social Security number**
- **License plate**
- **VIN** (vehicle identification number)
- **IP address**
- **Username**
- **Address**
- **Business name**
- **Cryptocurrency wallet**
- **Credit-card number**
- **Coordinates** (latitude/longitude)
- **Keyword** (the fallback when nothing else matches)

A crucial caveat about that classifier: its "confidence" is confidence that your *input looks like* an email or a phone number. It is **not** confidence that the *results* actually belong to the person you meant. There is no person-match confidence score. Nova can be very sure "this is a phone number" and completely wrong about whose life it then shows you.

13.5 The data sources: what Nova searches across

A single Nova search fans out to many separate data sources. Each one is a different database with its own endpoint in the code. Here is the core set, in plain language:

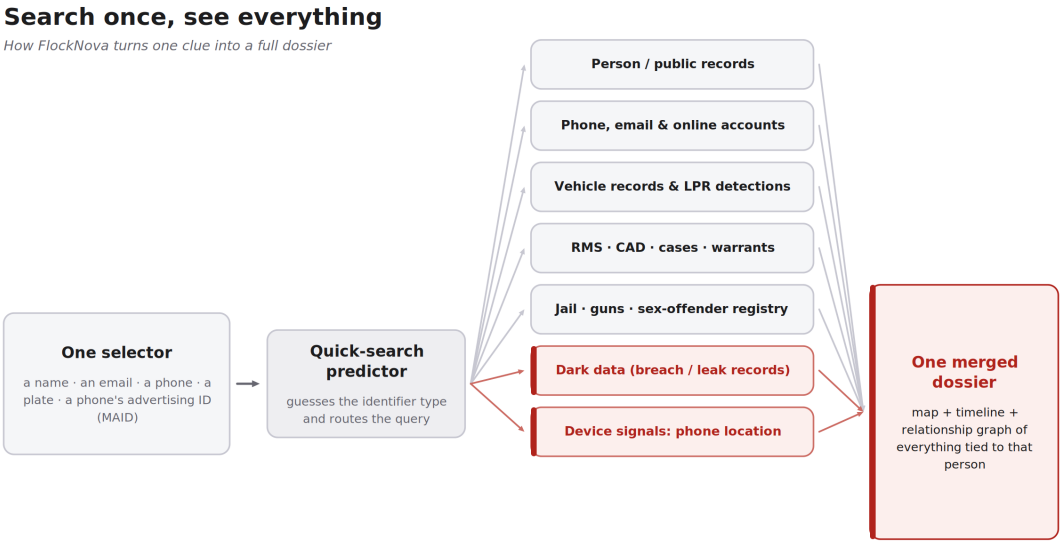


Diagram: author's illustration, based on FlockNova's search predictor and data-source endpoints.

Source	What it searches / returns
Person / public records	Identity records: names, dates of birth, phones, emails, addresses, SSNs
Phone data	Records tied to a phone number
Email data	Records tied to an email address
Online accounts	Accounts linked to an email, phone, or username
Dark data	Breach/"dark-web"-style records (see 13.9)
Address	Address records and who is tied to them
Device signals	**Phone-location** records tied to an email, device ID, or advertising ID (see 13.7)
IP signals / WhoIs	Location and intelligence tied to IP addresses
Location signals	Devices seen within a drawn geographic area (see 13.7)
Places of interest	Businesses and locations
Vehicle / LPR	Vehicle records and Flock license-plate-reader detections

Source	What it searches / returns
RMS person / vehicle / arrest	Police records-management data: people, vehicles, arrests
CAD / cases / warrants	Dispatch events, case files, warrants
Body-worn camera	Officer body-cam event metadata
Sex offender registry	Registered-offender lookups
Guns / inmates / property	Firearm records, jail/custody records, property items
Human trafficking / ICAC	Specialized anti-trafficking and internet-crimes-against-children leads

13.6 Everything Nova can find *about* you

When those sources return results, Nova collects them into a shared workspace with dozens of categories. Assembled, the picture Nova can build about a single person includes:

- Names, aliases, ages and dates of birth, and deceased status;
- Social Security numbers (where data-sharing flags allow display);
- Current and historical **addresses**;
- **Phone numbers** and **email addresses**;
- **Online usernames and accounts**;
- **Relatives and associates**;
- **Vehicles, plates, and VINs**, and vehicle **owner** records;
- Police records: physical descriptors (height, weight, race, ethnicity, hair, eyes, build, **scars/marks/tattoos**, gang affiliation, driver's license), **arrests** (and the arresting officer), **cases**, **CAD events**, **warrants**, and **body-cam** event metadata;
- **Inmate/custody records**, including FBI and NCIC numbers and booking dates;
- **Guns** and **property items**;
- **Criminal history:** charges, courts, pleas, dispositions, sentences, fines, and mugshots;
- **Breach/"dark" records** tied to your identifiers;
- **Device-location signals:** coordinates and timestamps of where a phone associated with you has been;
- **Mobile advertising IDs** and device records;
- **IP address** and WhoIs data;

- Cryptocurrency-wallet and credit-card mentions.

That is not a plate lookup. That is a dossier.

13.7 How Nova tracks phones: signals, MAIDs, and de-pseudonymization

This is the most invasive capability, and it deserves careful explanation because it is how a phone becomes a location trail.

Modern phones and apps constantly generate location data tied to identifiers, most importantly the **MAID** (Mobile Advertising ID), a unique code advertisers use to track a device, plus app "registration IDs," hashed emails, and IP addresses. This data is bought and sold in the location-data industry. Nova is wired to search it. Its device-signal endpoints let an investigator go from an identifier to a set of timestamped GPS coordinates:

- **Email → locations:** give an email address, get location signals for devices tied to it.
- **Advertising ID (MAID) → locations:** give a mobile advertising ID, get its location history.
- **Registration ID → locations:** give an app registration ID, get its location history.
- **Hashed email → device:** resolve a hashed email to a device.
- **IP address → signals:** get device signals tied to an IP.
- **Geographic area → devices:** draw an area on a map and get **every device that appears inside it**: a reverse-location or "geofence" search that starts from a place, not a person.

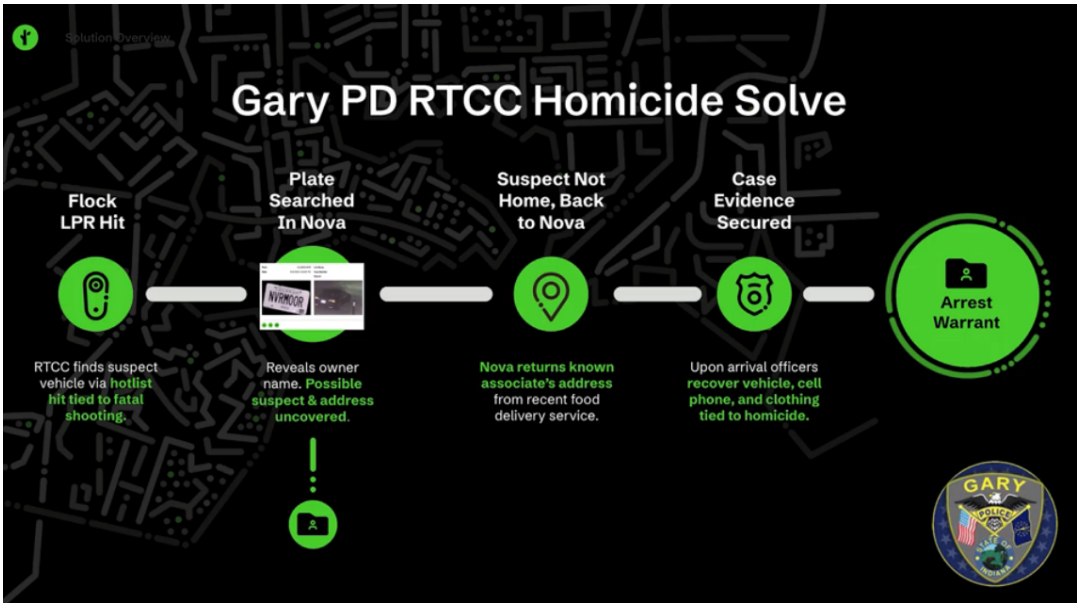
The location records Nova reads carry a **timestamp, a registration ID, an IP address, and latitude/longitude.** And Nova can **de-pseudonymize** these: it has endpoints that turn a registration ID into a **mobile advertising ID** and into a **device record**, walking from an anonymous-looking identifier to a specific device and, joined with the identity sources above, to a named person. This is not a description of what such a system *could* do; it is what Nova's own code does, calling an endpoint literally named `getMaidFromRegistrationIds` (with a companion `getDeviceFromRegistrationIds` that resolves the same identifier straight to a device record):

```
    console.log("Getting MAID from registration ID:", e.registrationId));
  let S = { registrationIds: [e.registrationId] };
  try {
    const x = await Kt.post("/v2/device/getMaidFromRegistrationIds", S);
    t({ ...e, advertisingId: x.data.advertisingId });
    const y = r.signals.map((C) =>
      C.registrationId === e.registrationId
        ? { ...C, advertisingId: x.data.advertisingId }
        : C,
    );
    n({ ...r, signals: y });
  } catch (x) {
    console.error("Error fetching MAID:", x);
  } finally {
    v(!1);
  }
};
```

Two features make this genuinely a tracking tool:

- A **“Follow Device”** mode with a **90-day default** window when no dates are entered.
- A **multi-area** mode that looks for the **same device across two to five drawn areas at once**, each defaulting to a **250-meter** radius: the pattern you would use to test “is the phone that visits this address also the phone that visits that clinic, that workplace, and that meeting spot.” These area searches are not limited to a place and a radius; the form also accepts a **day-of-week and time-of-day** filter, so the question narrows from “which devices appear here” to “which device is here on weekday mornings.”

This is the reality behind the phrase people use, that Nova can be handed the email or identifier tied to an app on a phone and return **where that phone has physically been.** And it is not hypothetical: Flock’s *own* sales material walks through a case where, after a plate hit and a Nova search, **“Nova returns [a] known associate’s address from [a] recent food delivery service.”** In other words, the food-delivery example is Flock’s own example.



The endpoints to do all of this are in the code, and none of them visibly require a case number or a statement of legal authority.

Where does this phone data even come from? This is the question most people should ask, and the answer is the quiet scandal of the whole feature. Flock's cameras do not collect this location data. It comes from the **commercial location-data industry**: your advertising ID and your GPS coordinates are harvested by ordinary apps on your phone (weather, games, shopping, delivery, and many others) through advertising software kits, then aggregated and sold by data brokers. Nova is wired to query that market. The examined software does not reveal which broker or app the data came from, what consent (if any) you gave, how accurate it is, or how often it samples. In plain terms: **your movements can become searchable by a government user not because you were ever suspected of anything, but because an app you installed sold your location.** The U.S. Federal Trade Commission has taken enforcement action against exactly this pipeline, app makers and brokers collecting and selling precise phone-location data, which shows the industry path is real even though it does not name Nova's specific supplier. The provenance, the consent, and the legality of that data are exactly the things the code cannot prove, and exactly the things that matter most.

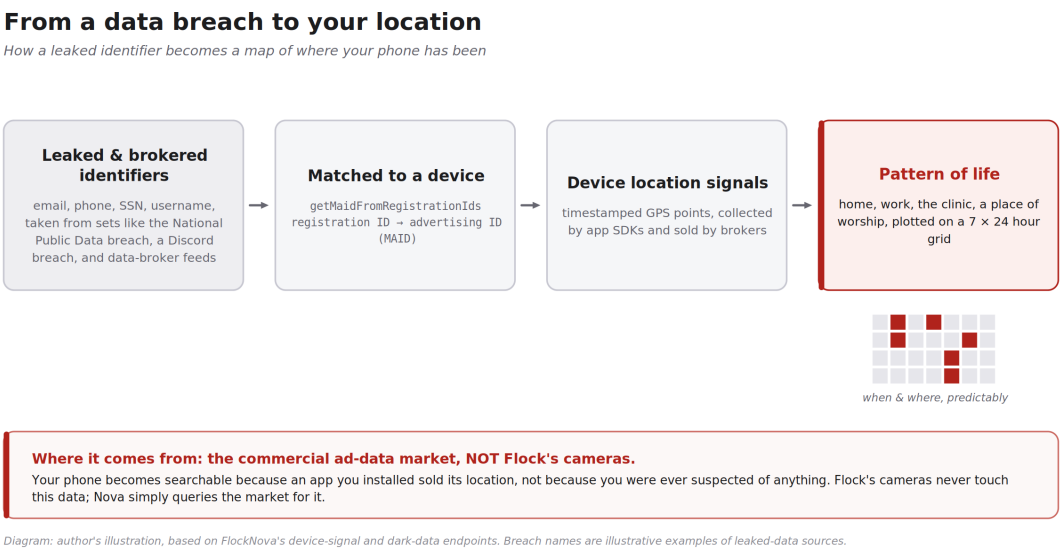


Diagram: author's illustration, based on FlockNova's device-signal and dark-data endpoints. Breach names are illustrative examples of leaked-data sources.

13.8 Bulk signals, heatmaps, and pattern-of-life

Nova does not only look up one device at a time. It has a **bulk signals** capability: it can load a large export of location signals, up to **500,000 rows** at once, into the browser, then plot them on a map as points, group them by device (registration ID), and derive the unique devices, unique IPs, and time ranges present. This is mass location analysis, not a single lookup.

On top of that sits a timeline-and-heat view Nova calls **TimeHeat**. It gathers timestamped events from many sources at once (camera scans, phone signals, bulk signals, police cases, dispatch events, LPR reads, and arrests) and lays them on a shared timeline. It also builds a **7-by-24 day-of-week by hour-of-day grid**: click a cell (say, “Tuesdays at 8 a.m.”) and it filters everything to that pattern. That is a **pattern-of-life** engine. Its entire purpose is to surface routines: when and where a person or device predictably is.

A person record also has a **Location History** tab that maps their historical addresses and can drop straight into **Google Street View** of a selected address, and a **“What’s Here”** function that takes any address on the map and runs it back through the people search to return **who is associated with that location** (“Get People”). Address to people, people to devices, devices to pattern of life: the tool is built to travel in every direction.

13.9 Dark data: the “dark web” question

Nova contains a data source its own code labels **“Dark Data.”** The source is defined right there in the application: an adapter with `key: "DarkData"`, `permissionKey: "hasDarkDataAccess"`, `resultKey: "darkDocs"`, and an endpoint `dark/getExtDarkData`, whose request can carry an email, first and last name, city, state, keyword, username, phone, **SSN**, IP address, **crypto wallet**, and **credit-card number**.

```
key: "DarkData",
icon: lG,
label: "Dark Data",
permissionKey: "hasDarkDataAccess",
resultKey: "darkDocs",
endpoint: "dark/getExtDarkData",
getPayload: (e) => {
  const {
    email: t,
    firstName: n,
    lastName: r,
    city: o,
    state: i,
    keyword: s,
    searchTerm: l,
    username: a,
    phone: c,
    ssn: u,
    ipAddress: d,
    crypto: h,
    ccn: p,
    searchType: f,
```

Its dedicated search screen lays the categories out as plain tabs: **Keyword, SSN, Email, IP Address, Crypto Wallet, Credit Card Number, Discord Channel, Telegram Channel,** and User. Results come back with fields like **crawl date, network, leak name, leak host, and a download location**, and one component even ships a large hard-coded dictionary mapping breached domains to occurrence and risk scores. This is the vocabulary of breach and leak data, not public records.

This collides directly with Flock’s public position. After reporting in 2025 raised concerns about breached data in Nova, Flock publicly stated that Nova would **not** supply dark-web data purchased from known breaches or stolen data, and would instead

use public records, OSINT, LPR, RMS, CAD, jail, and agency-shared data. Independent analysis of Nova's code (by this author and others) pointed at exactly this "Dark Data" source and its breach-style fields as evidence in tension with that denial.

The honest resolution is an unresolved contradiction, stated as such: **Nova's code contains a breach/"dark" data capability with leak-oriented fields; Flock's public statement denies supplying dark-web/breach data.** The code cannot prove where the data ultimately comes from (a genuine breach, a broker, a paste site, or a licensed feed). Both facts are real; neither erases the other. What is not in dispute is that the *capability* to search breach-style data by SSN, card number, and messaging-app channel was built into the tool.

13.10 Ava: the AI assistant

Nova includes an AI chat assistant named **Ava** ("Automated Virtual Assistant"), shown to users whose account has an "AI access" flag. You type a plain-English request and Ava interprets it and can run searches for you. The example prompts it advertises are revealing: *"map 911 calls over the past 30 days," "return all available information about a phone number," "map all homicides over the past year."*

Ava sends your text to a backend AI, which returns an interpreted intent, a visualization type, and any **extracted identifiers**, plus a flag for whether it has "enough data" to proceed. When that flag is set, Ava can **automatically run searches without a second confirmation.** In the captured build, its live branch takes an email address Ava pulled from your prompt and immediately runs both a person search and a dark-data search on it. As with the rest of Nova, the AI request carries **no case number, purpose, or legal-authority field.** Natural-language in, investigative searches out.

13.11 The specialized modules

Beyond person search, Nova carries a set of specialized, often staff-gated modules that show the breadth of its ambitions:

- **Gun and inmate search:** firearms by make/model/caliber/serial/owner; inmates by name, physical description, SSN, aliases, FBI/NCIC numbers, and booking dates.
- **Public criminal history:** nationwide public criminal records built from a person's identifiers, with an explicit warning that results "may not relate to the current entity" and require verification.

- **CompStat and gun-crime dashboards:** crime-statistics dashboards, one of which fuses ballistics data with **device-location signals**, extracting device registration IDs from location areas and linking them into an investigation.
- **Real Estate leads:** a module that pulls **mortgage-recorder data** by county and loan amount and can send recurring reports to customers.
- **ICAC / trafficking dashboards:** specialized modules for internet-crimes-against-children leads (by username, IP, channel, country) and anti-trafficking business analysis.
- **Aerodome flights:** search drone flight logs by area and time, returning paths, altitude, and telemetry.
- **Census, map overlays, and organization layers:** demographic and geographic enrichment layered onto the map.

13.12 Who's allowed to see what

Nova's permission model is a set of flags carried in the user's login token (`hasPersonDataAccess`, `hasDarkDataAccess`, `hasSignalDataAccess`, and so on) plus per-organization feature switches. These control which tabs and sources a given user sees. But the evidence is blunt about their strength: **these are client-side, advisory gates.** They decide what the browser *shows*; they are not, by themselves, a security boundary. Real enforcement would have to happen on Flock's servers, which cannot be seen from the outside, and the client itself has bugs and misspellings in these gate names that can make a control silently do nothing. The examined code also shows the login token, and in some flows a body-cam video's access token, being handled and logged in ways that expose them.

Nova does carry some governance surfaces worth acknowledging: its legal banner restricts using the underlying (Lucidus) data for credit, insurance, housing, or employment eligibility decisions (a nod to the federal Fair Credit Reporting Act), warns that public-record results may not describe the intended person, and includes an opt-out / redaction request path. Those are real, but they are notice and remedy at the edges; they do not add the enforced, per-search authorization the sensitive parts of the tool lack. I have attempted to use the opt-out path and was denied.

Part 14: Officer apps, phone scanners, and the officer-versus-civilian line

Flock does not only live on poles. It runs on officers' phones and watches, and this creates a privacy distinction that is easy to get wrong.

The operator app (internally "Sweetwater") gives officers hotlist and audio alerts, plate lookup, and image verification. It also turns the phone itself into a scanner: a **run-plate** feature uses the phone's own on-device AI to read a plate through the camera and check it against hotlists. Any patrol phone becomes a mobile plate reader, so plate collection is not limited to fixed cameras; coverage expands wherever an officer points a phone. Alerts also reach Apple Watch and Wear OS.

Two things about this matter for privacy, and they cut in opposite directions:

- **The officer app tracks the officer.** It carries shift state and foreground/background location, and the code shows a push message that can prompt the phone to report its current latitude and longitude. That is genuine location tracking, of the officer and their device. How often it fires, who can see it, how off-shift time is handled, and how long it is kept are not clear from the outside.
- **It is not the officer app that tracks the public.** A common and understandable fear is that the officer app is quietly following civilians' phones. It is not: that capability is a different product entirely, namely Nova's device-signal workflows (Part 13.7). Keeping these apart keeps criticism accurate. The officer app is officer telemetry. Nova is where a member of the public's phone becomes a location trail. Both are real; they are not the same thing.

Part 15: The privacy problems, in depth

Everything up to here describes what the system *can do*. This part is about *harm*: the concrete ways it can hurt ordinary people, most of it without anyone breaking a single law of computer security.

15.1 Sensitive places, and the reverse-location dragnet

The most under-appreciated risk is that **a place can be a proxy for a private fact.** Two of Flock's search modes begin with a location instead of a suspect:

- **Multi-Geo** (classic Flock) finds every vehicle that appeared at Place A during one time window *and* Place B during another.
- **Multi-area device-signal search** (Nova) finds every phone that appeared inside two to five drawn areas.

Point either of those at a reproductive-health clinic, a house of worship, a protest or picket line, a union hall, a domestic-violence shelter, a school, an immigration office, a recovery meeting, or the corner where a journalist met a source, and the "candidate list" becomes a list of people whose mere presence reveals something they never chose to disclose. Everyone unrelated who simply happened to be there is swept in alongside the target. And because the phone-area search can be narrowed by day of week and hour, the dragnet is not even limited to "who was here once"; it can ask "who is here every Tuesday morning," turning a single sensitive visit into a detected routine. Nothing in the examined software blocks sensitive locations, requires special approval to search them, or minimizes the bystanders. The only thing standing between this capability and abuse is an operator's own policy and restraint.

15.2 Wrong matches and guilt by association

Flock joins data of wildly different quality (a machine-read plate, a stale registration, a years-old breach record, two cars on the same road at the same time) and Nova has **no person-match confidence score.** So a search can confidently return the *wrong* person: a shared name, a recycled phone number, an old address, a cloned plate, or a car that merely drove the same route. Worse, Nova's link expansion is **on by default** (Part 13.6): one lookup can silently pull in relatives and associates, so a person can land in an investigative graph not for anything they did but for who they know or where they drove. Nova's own legal banner concedes the danger: results are "investigative leads" that "cannot themselves constitute probable cause." The harm arrives when that caution is ignored and a bad match taints a traffic stop, a search, an arrest, or a warrant affidavit built on top of it.

15.3 Your data leaving to third parties

Flock's own applications wire in outside analytics and monitoring services, and sensitive data can travel with them. In the captured hotlist app, instrumentation from services such as **FullStory, Segment, and Datadog** is present and is capable of capturing what users type and click (which can include **plate numbers, owner notes, and search terms**) and sending it to third-party vendors. Nova likewise ships product-analytics identifiers (user email, name, selected agency) to an outside tool, and the examined code handled access tokens carelessly in places (for example, a body-camera video's access token placed directly into a stream URL that then gets logged, and an API token displayed on screen and copied to the clipboard). The point is blunt: **sensitive investigative data does not necessarily stay inside Flock.** Some of it flows out to analytics and logging providers whose own retention and use are hard for anyone to see.

15.4 External map providers

A smaller but concrete leak: when a Nova investigator maps a person's address history or uses "What's Here," the selected address is handed to outside mapping providers: **Mapbox**, and **Google** for geocoding and Street View. Those companies receive the addresses an investigator is interested in, and whatever they retain or infer from that is outside Flock's system entirely.

15.5 The durable-copy problem

"It deletes after 30 days" is one of the most misleading comforts in this field. It helps to think in terms of **four kinds of copies**, because deleting one does not delete the others:

- the **source** observation (the original camera read, call, or signal);
- the **derived** data made from it (the OCR text, the extracted attributes, the transcript, the alert, the graph edge, the heat aggregate);
- the **investigation** copy (anything added to a case, note, saved search, report, or evidence package); and
- the **downstream** copy (an exported CSV, image, PDF, screenshot, clipboard grab, mobile cache, or a copy already sent to another agency).

A 30-day deletion typically touches only the first. The record can persist in all the rest: evidence packages, hotlist notes, Nova investigations, another agency's systems after a share, records-management attachments, audit logs, search history, backups, and browser caches. Revoking a share inside the product does not recall a file someone

already downloaded, and correcting a wrong registered owner does not retract the alert that already went out. Nova also exposes plain copy-to-clipboard actions for identifiers and coordinates, which create a copy that no export record or audit log ever sees. The right question is never only "what is the retention setting" but **"which copies exist, who holds each one, and what actually deletes it."**

15.6 What "tracking" precisely means

"Tracking" is not one thing, and being precise about it is what keeps the criticism credible rather than dismissible. There are five distinct modes, and they carry different technical and legal weight:

Mode	Plain meaning	Flock example
Historical query	Search records after the fact	Plate search, FreeForm, Nova signals
Correlation / reconstruction	Stitch discrete hits into a route or dossier	Convoy, Multi-Geo, Nova graph and TimeHeat
Alerting	Notify when a new event matches a target	Hotlist hit, person-detection alert
Live operational location	See where an asset is right now	Officer-app location, 911 caller location, patrol AVL
Continuous identified-person tracking	Persistently follow one named human	Not established as a general Flock camera product

Flock's public position bans "tracking of individuals" and frames its cameras as vehicle-focused. That coexists with FreeForm's descriptive people search, real-time alerts, FlockOS's movement-oriented language, and Nova's phone-signal trails. The honest reconciliation: **dense discrete observations, plus correlation, plus identity fusion can reconstruct a person's movements even if no single feature is labeled "follow this human."** The reconstruction is the whole point. It is why "we do not track individuals" and "you can rebuild someone's week from our data" can both be literally true at the same time.

Part 16: The law, the Fourth Amendment, and accountability

This section spots the issues; it is not legal advice. But an informed reader should know where the legal lines fall.

A case number is not a warrant, and the Constitution never asked for one. The Fourth Amendment forbids *unreasonable* searches; it does not say "enter a case number." So Nova letting a search run without a validated case number is an **accountability** failure, not automatically a constitutional violation. The reverse is also true: a filled-in case field proves nothing about legality. The real problem, restated, is that the software provides no reliable way to tell a lawful search from an unlawful one: they look identical to the system.

Phone-location data is where the constitutional stakes are highest. In *Carpenter v. United States* (2018), the Supreme Court held that the government acquiring historical cell-phone location from a third party is a Fourth Amendment search that generally requires a warrant. In *Chatrie v. United States* (decided June 29, 2026), the Court held that obtaining the historical location history at issue was a search **even for a window as short as two hours**, and even though a company was holding the data. The plain implication for Nova: **if its device-signal searches return historical phone location and a government user runs them, that acquisition is very likely a Fourth Amendment search**, one that a self-assigned "case number" does nothing to satisfy.

License-plate networks are less settled. No single Supreme Court case cleanly resolves long-term, nationwide license-plate surveillance. The guiding signals are *United States v. Jones* (2012, long-term GPS tracking raised serious constitutional concern), the "mosaic" idea that enough individually harmless observations become a search in the aggregate, the Fourth Circuit's *Leaders of a Beautiful Struggle v. Baltimore Police* (persistent aerial surveillance was a search), and state decisions like *Commonwealth v. McCarthy* (Massachusetts), which upheld limited plate-reader use on its facts while warning that a dense enough network could cross the line. The legal risk climbs with duration, camera density, cross-jurisdiction sharing, reverse-location searching, sensitive places, exports, and, above all, fusion with identity and phone data. That last factor is exactly what Nova adds to the plate network.

The accountability gap ties it together. A system this powerful is only as safe as its controls, and the controls examined here are weak: case numbers that are optional and unvalidated, audit logs that fail open or are skipped on the most sensitive actions,

permission gates that are advisory rather than enforced, and data that can leave through exports and third-party tools. Strong external oversight, including warrant requirements for phone-location and sensitive searches, enforced and complete audit logs, retention limits that reach *every* copy, protected-place rules, and independent review of inter-agency sharing, is not a nice-to-have here. It is the difference between “a tool for solving specific crimes” and “a searchable record of everyone’s movements.”

Part 17: Putting it together, from one camera to a pattern of life

Here is the whole system in a single walk-through, because the danger is not in any one feature. It is in the sequence.

1. **A camera sees a car.** An ordinary Falcon on an ordinary road records a plate, a vehicle fingerprint, a direction, a time, and a location. The car’s owner did nothing but drive to work.
2. **The record becomes searchable and alertable.** That detection can be found later by plate, partial plate, or vehicle description, and, on video-enabled cameras, by a plain-English FreeForm query. It can trigger a standing alert if the plate is on a hotlist or matches a saved search, and a drawn ROI can mark the exact lane it was in.
3. **It joins the map.** In FlockOS the detection sits beside patrol cars, 911 calls, drone feeds, and other agencies’ shared cameras, comparable to everything else because they share a time and a place.
4. **It becomes a person.** In Nova, the plate leads to the registered owner, and the owner’s name leads out across public records, addresses, phones, emails, online accounts, relatives, arrests, and breach data.
5. **It becomes a movement history.** The owner’s email or a phone identifier leads into device signals (timestamped coordinates), and Nova’s bulk-signal, TimeHeat, and multi-area tools turn those into a routine: home, work, the places visited on Tuesdays at 8 a.m.
6. **It becomes intelligence.** Convoy and multi-geo analysis reveal who travels with them. “What’s Here” reveals who else is tied to their address. The day/hour heat grid reveals the rhythm of their life.

At no point in that chain did the person do anything but exist in public. And at several points (the phone tracking, the dark data, the AI-driven searches) the tool did not require a warrant, a case number, or a stated reason to proceed.

That is the system. The cameras are the doorway; the fusion is the room.

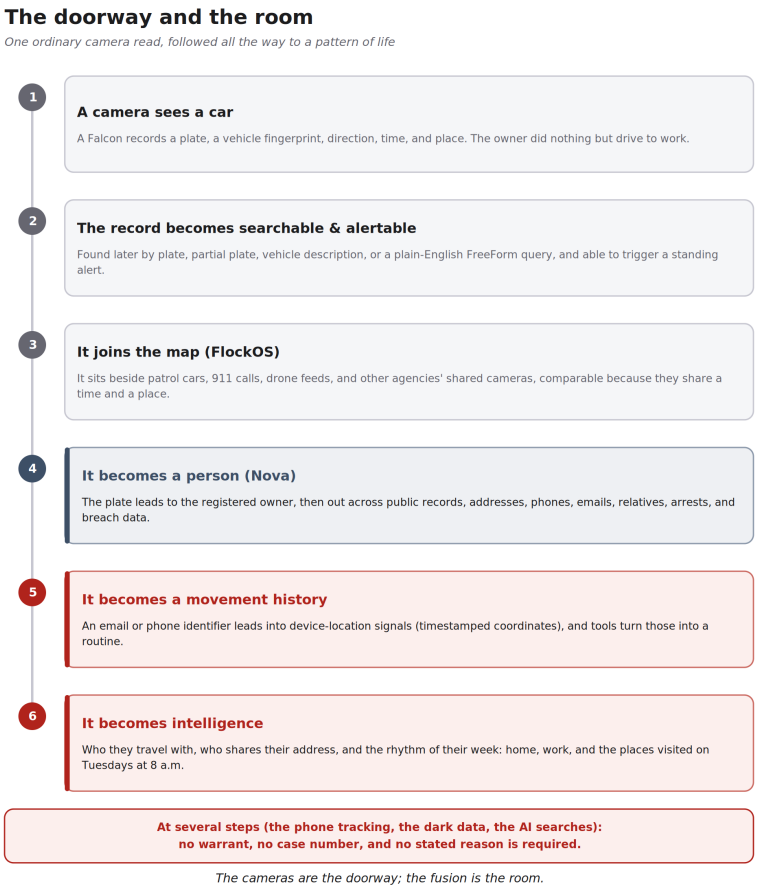


Diagram: author's illustration summarising Parts 13–17 of this guide.

Part 18: Why the security failures matter

This guide is a companion to a technical disclosure documenting four security failures in Flock's own systems, reported to the company between June and December 2025. In brief, they were:

1. A **production mapping credential** (an ArcGIS key) hardcoded and published dozens of times in public developer files, tied to premium geospatial and routing capabilities.

2. **Flock's own application code served before login**, exposing the blueprint of Search, Hotlist, and FlockOS: endpoints, permissions, and data models.
3. A **credential factory**: services that handed out production mapping credentials to anonymous, unauthenticated callers.
4. **Nova's application code served before login**, exposing the entire data-fusion blueprint described in Part 13.

There is also an **integrity** dimension that is easy to overlook. Some of the mapping layers were not read-only; a production camera service advertised create, update, and delete capabilities. The risk of a badly secured surveillance map is therefore not only that an outsider can *see* where collection is; it is that the map police rely on as ground truth could be *altered*: camera positions moved, statuses flipped, records deleted, or false markers added. A surveillance system that can be quietly edited is arguably more dangerous than one that can only be read.

These failures are why so much of this guide can speak with confidence about *what the code shows* rather than only *what Flock says*. They also carry their own lesson: a system that concentrates this much surveillance power over this many people is only as trustworthy as its security and its accountability, and both were found wanting. When a single platform can track vehicles nationwide, absorb third-party cameras, fuse identity and phone-location data, and do it without reliably enforced warrant or purpose controls, its security stops being a private corporate matter and becomes a public-safety and civil-liberties one.

Part 19: Common misconceptions

The corrections below are the ones that matter most for an ordinary reader. Each is written as the common belief, the reality, and why the evidence supports it, keeping the guide's discipline of separating what Flock markets, what the code shows, and what is analytical interpretation.

Myth: "Flock is just cameras that read license plates." Reality: Cameras are only the first of three layers. The plate reader creates a searchable record that also captures the vehicle's appearance, direction, time, and location; that record feeds real-time alerts, live video, and cross-agency sharing; and FlockNova fuses it with identity and phone-location data to build a dossier and a movement history. **Why:** The device list, the six

search modes, the sharing permissions, and Nova's data-fusion endpoints are all visible in Flock's own code, not just its marketing. "Just plates" is the marketing scope; the title of Flock's own patent calls it a "dynamic surveillance network."

Myth: "Flock's plate-reader cameras don't capture anything about people." Reality: Flock's plate-reader FAQ does say that line is "vehicles, not people" and uses no facial recognition. But its video-camera line ships people-detecting AI (Guardian Mode, People Detection Alerts, FreeForm), and Flock has announced that *every* plate reader will become a video camera at no cost. The capability disclaimed for one product is standard on the product the first is being converted into. **Why:** Both FAQs are Flock's own public marketing; the "all LPR become video cameras" release is a captured company-event statement. The tension between them is documented, not inferred.

Myth: "FreeForm is facial recognition." Reality: FreeForm searches by *appearance* (clothing, visible accessories), returns candidates for a human to review, and Flock says it uses no biometrics. Separately, Flock's *patent* describes true facial recognition and race/sex/height/weight profiling, and the examined software does not show face-matching running. All three statements are true and must be kept apart. **Why:** FreeForm's non-biometric description is marketing plus visible code structure; the facial-recognition capability is in the patent; "not currently deployed" is the analyst's reading of the examined code. Collapsing them in either direction misleads.

Myth: "A hotlist hit means the car is stolen or the driver is guilty." Reality: A hit means a camera's software matched a string on a list. It can be a misread plate, a cloned plate, a sold or rented car, or a stale entry. Flock's own screen says custom hotlists "should never be used as probable cause." A hit is a reason to look, not to stop, search, or arrest. **Why:** The probable-cause disclaimer is quoted from Flock's own interface; the failure modes are the normal behavior of automated matching, grounded in the code's OCR and partial-plate handling.

Myth: "Anyone on a hotlist must have done something to get there." Reality: Adding a plate to a hotlist is an administrative act. The case-number and reason fields are optional and unvalidated, and nothing in the examined software prevents an operator from listing an arbitrary, innocent person's plate, for any reason or none, with no review, mandatory expiration, or notice to the person. **Why:** The optional, unvalidated hotlist fields are visible in Flock's code; the absence of preventive controls is what the examined software shows and what this author observed when trying the opt-out path.

Myth: “If there’s no warrant or case-number field, the search must be illegal.” Reality: Legal authority lives outside the software. A missing or empty case number is an accountability gap, not automatically a crime. But some searches, especially historical phone-location, very likely *do* require a warrant under *Carpenter* and *Chatrie*, and the software cannot tell you whether one exists. **Why:** Constitutional analysis applied to the code’s finding that case numbers are optional and unvalidated.

Myth: “Nova’s phone-location data comes from Flock’s cameras.” Reality: It does not. The device signals come from the commercial location-data market: advertising IDs and GPS coordinates harvested by ordinary apps and sold by data brokers. Your phone can become searchable because of an app you installed, not because a camera saw you. **Why:** Nova’s signal endpoints and the MAID de-pseudonymization call are in the code; the data-broker provenance is the established industry pipeline the FTC has acted against. The code does not name the specific supplier, which is itself part of the problem.

Myth: “A 30-day deletion means nothing lasting exists.” Reality: A 30-day deletion typically touches only the original footage. Exports, investigation files, hotlist notes, alerts, audit logs, and anything already shared to another agency are separate copies with their own lifespans, and revoking a share does not recall a file someone already downloaded. **Why:** The paid multi-year retention tiers are in Flock’s price list; the “four kinds of copies” is a framework for reasoning about what deletion actually reaches.

Myth: “A Flock camera in my town only serves my town.” Reality: Flock is one shared national platform. Sharing is a setting, not a default: an agency is not required to share its reads beyond its own cameras, but many choose to, making them discoverable or shareable across other agencies, up to nationwide. Third-party cameras absorbed through Wing gateways stretch the searchable universe well past Flock’s own poles. **Why:** The sharing and discoverability settings and the gateway integrations are in the code and the device list.

Myth: “Only the police use Flock.” Reality: Flock’s own software enumerates HOAs, property managers, businesses, schools, and channel partners as customer classes. A private HOA or business can run plate readers around your home or workplace and choose to share that data with police. **Why:** The customer-class enumeration is in Flock’s code.