Flock Cameras, Faces, Gait, and the Fusion That Ends Privacy in Public

Gregory M. Galvin
Galvin Law Group, LLC · Bluffton, South Carolina
August 29, 2026

The government generally needs a warrant to reconstruct a person's movements from a phone. A Flock network is the same dump—of every car—already sitting in a vendor cloud.

Abstract

The public fight over Flock Safety's automated license-plate readers is real, and some of the anger is earned. It is also the wrong unit of analysis. The cameras that photograph cars are one sensor in a stack that already includes facial recognition, video that follows pedestrians, commercial phone-location dossiers, search and marketing databases, and computer-vision tools that can infer gait, injury, body change, and—soon enough—affect. Each stream can be defended, in isolation, as "public," "anonymized," or "not facial recognition." Fused, they reconstruct the person. After *Carpenter v. United States*, the government generally needs a warrant to pull historical cell-site records that reconstruct a person's movements. A tower dump—every phone that touched a cell site in a window of time—is the same architecture aimed at everyone who was there. A Flock network is that dump, already built, sitting in a vendor cloud, searched without asking a judge. The Fourth Amendment still treats many of these tools as if an officer were standing on a sidewalk with a notepad. That doctrine will not hold the line. Online privacy is already largely gone. If the physical-world stack is allowed to mature under the same legal lag, privacy in public will follow.

I. The fight we are having

Flock Safety did not invent the idea of photographing a license plate. It industrialized it. The company sells solar-powered automated license-plate readers and a national network that lets thousands of agencies search vehicle images—plate, make, color, and other "vehicle fingerprint" traits—across jurisdictions. Reporting in 2026 put the scale in the tens of billions of plate scans a month. Police credit the network with finding stolen cars and missing people. Cities have also cancelled or paused contracts. Officers have been accused of using the system to stalk former partners. Investigative reporting has described federal immigration access through local agency logins even where Flock says it has no direct ICE contract.[1a] In August 2026, after months of bipartisan backlash, the company announced that previously optional audit tools would become mandatory and that agencies would get tighter controls over how others search their cameras.[1]

That controversy is easy to see. A camera on a pole is a political object. A town-hall slide that says "license-plate reader" is something a city council can vote on. "No facial recognition" is a sentence a vendor can put on a trust page, and Flock does. Its public FAQ states that Flock cameras "do not use facial recognition technology," that searches are "based on vehicle characteristics, and not identity," and that Flock "cannot recognize, identify, or track individuals."[2]

Take that sentence seriously, and then notice what it does not say.

It does not say the camera never photographs a face. It does not say a different Flock product—the Condor pan-tilt-zoom camera—cannot acquire a pedestrian and follow the person down a path. InvestigateTV's June 2026 reporting showed Condor units doing exactly that, and Flock training material describing cameras that "acquire and track that person as they walk."[3] It does not say an officer cannot type a clothing description into a video-search tool and pull hits across a network. It does not say the plate hit cannot be joined, five minutes later, to a Clearview search, a data-broker location history, a Google warrant, or a marketing segment. And it does not say the law treats that join as one search.

The public is angry at the pole. The pole is not the system.

II. The fight we are not having

Facial recognition is not a hypothetical. It is a product. Clearview AI markets a law-enforcement search against a database it has described as tens of billions of publicly scraped images. Police use it after the fact: upload a still, get candidate faces, investigate. Other vendors sell live or near-live matching against watchlists. Airports, stadiums, stores, and schools have all deployed some version of the same idea. The legal and political fight over Clearview, over school-camera face matching, and over real-time street identification has been running for years. Flock's "we don't do faces" claim is a product-line statement, not a description of the surveillance market.

A face is only the most famous biometric. Computer vision already estimates identity and condition from the rest of the body. Gait recognition—identifying a person by how they walk—works at a distance, through a hat, and without the subject looking at the camera. The same video that shows a limp, a walking boot, or a cast is medical inference whether or not anyone labels it "health data." Research systems estimate body-mass change from ordinary images. None of this requires a science-fiction leap. It requires a camera good enough to film a sidewalk and a model cheap enough to run in the cloud. Those already exist.

Emotion recognition is the next layer, and it is not waiting for a breakthrough. Commercial systems already claim to score faces and voices for happiness, anger, attention, and stress. The European Union treated that risk as real enough to prohibit emotion-recognition AI in workplaces and schools under the AI Act, with only narrow medical and safety exceptions, beginning in February 2025.[4] The United States has no equivalent national ban. If a street camera can already say "this is the same person who drove the gray SUV last Tuesday," it is not a long step to "this person looks distressed," "this person looks like they gained weight," or "this person is favoring the left leg." Those inferences will be wrong often enough to ruin people and right often enough to be useful to whoever buys the feed.

The still deeper layer is not on the pole at all. It is the join.

Phone-location brokers have sold "patterns of life" to police for years. Fog Data Science's Fog Reveal product, built on app-derived advertising identifiers, has been marketed as billions of points on hundreds of millions of devices, cheap enough for a county sheriff. Venntel, Babel Street's Locate X, and similar firms have sold comparable telemetry to federal agencies. That data does not come from a cell-tower warrant. It comes from a weather app, a game, a coupon SDK—the same commercial exhaust that already powers online advertising. Google search history, YouTube watches, ad-tech segments, purchase histories, and social graphs are the rest of the dossier. *Riley v. California*, 573 U.S. 373, 134 S. Ct. 2473 (2014), already described modern phones as "minicomputers" that "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[5] The only new move is to stop pretending the street camera and the phone are different cases.

Online, that fusion has already happened. The person who uses a browser is, for practical purposes, known: identity, intent, income band, medical curiosity, political lean, 3 a.m. searches. The remaining argument is about how much of that dossier the government may demand, and how much private platforms may sell. In physical space we still perform a civic fiction—that walking down Main Street is anonymous because no one officer can remember every face. The cameras, and the models behind them, retire that fiction.

III. Why "it's just a plate" is a legal error

American search law grew up on a sidewalk. If you stand in public, the officer may look at you. If you drive, your plate is displayed by law. If you hand records to a bank or a phone company, older cases said you assumed the risk that the company would hand them to the government. Those rules—*United States v. Knotts*, 460 U.S. 276 (1983), for following a car on public roads; *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), for third-party business records—are the doctrinal reason a city attorney can stand up and say a Flock camera is "just like an officer with a notepad."[6]

The Supreme Court has already started to admit that the notepad analogy fails when the notepad is infinite.

In *United States v. Jones*, 565 U.S. 400 (2012), the Court held that installing a GPS tracker on a vehicle, and using it to monitor the vehicle's movements, was a search because the government physically occupied an "effect."[7] The more important words for this decade are in the concurrences. Justice Sotomayor wrote that GPS monitoring "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." The government can "store such records and efficiently mine them for information years into the future." Because the technique is cheap and quiet, it "evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[8] She asked the question the Flock debate keeps dodging: whether people "reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." Awareness that the government may be watching, she added, "chills associational and expressive freedoms."[9]

Carpenter v. United States, 585 U.S. 296 (2018), took that intuition and made it a holding for historical cell-site location information. The Court held that accessing seven days of CSLI is a search, and it refused to extend *Smith* and *Miller* to those records. (The first order produced records spanning 127 days; the Court said seven days was enough.) "Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier," it said, "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." Mapping a phone over 127 days "provides an all-encompassing record of the holder's whereabouts" and "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" When the government tracks the phone, "it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." The data are logged for everyone, not only suspects. "In no meaningful sense," the Court said, "does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." Acquisition of the records was a search. The government must generally get a warrant; the Court reserved case-specific exceptions such as exigency.[10]

That is the right description of a national ALPR network, a city of Condor cameras, a face-search engine, and a broker location file—if they are described together. Courts have often been asked to apply that description to one tool at a time, and they have often declined. The fusion claim in this essay is advocacy, not a holding.

Carpenter invited that refusal. The Court called its decision "a narrow one." It said it did "not disturb the application of *Smith* and *Miller*" or "call into question conventional surveillance techniques and tools, such as security cameras."[11] Flock's lawyers quote that sentence. So do city attorneys. It is the most important loophole in modern Fourth Amendment law, and it was written as judicial modesty. It is being used as a business model.

The Fourth Circuit, sitting en banc, showed what happens when a court looks at the program instead of the sensor. In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021), Baltimore flew planes that photographed the city and retained the imagery long enough to reconstruct movements. The appeal was from the denial of a preliminary injunction. The pilot had already ended; Baltimore had deleted most of the data; the court still reached the merits because some investigative files remained. Over three dissenting opinions, Chief Judge Gregory wrote that because the AIR program "enables police to deduce from the whole of individuals' movements," accessing its data "is a search, and its warrantless operation violates the Fourth Amendment." The plaintiffs, the court held, were "likely to succeed on the merits." AIR data, it said, was "more like 'attach[ing] an ankle monitor' to every person in the city." The court did not require perfect tracking. Multi-hour blocks over consecutive days, with weeks of daylight to work with, were "enough to yield 'a wealth of detail,' greater than the sum of the individual trips."[12]

A Flock network that logs every passing car in a metro area for thirty days, searchable nationwide, is not a notepad. A Condor that follows a pedestrian is not a security guard glancing up. A Clearview query is not a witness saying "I think I know that face." A Fog Reveal replay of who stood near a clinic is not a stakeout. Each can be analogized to something an officer might have done in 1983. Together they are

Baltimore's planes without the planes—plus a name, a medical inference, and a marketing file.

Kyllo v. United States, 533 U.S. 27 (2001), is the other half of the warning. The Court held that using a thermal imager not in general public use to explore details of a home that would have been unknowable without physical intrusion was a search. The point was not heat. The point was that to withdraw the home's minimum privacy "would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[13] Gait, body-mass change, and affect are thermal imaging for the sidewalk: inferences about the body's interior, drawn from energy the body cannot help emitting in public. The current doctrine says the sidewalk is different from the home. The technology does not care.

IV. A Flock query is a tower dump the government already owns

The cleanest way to see the legal error is to stop analogizing Flock to a cop with a notepad and start analogizing it to a cell-tower dump.

A tower dump is a demand that a wireless carrier produce records of every device that connected to a particular cell site during a particular interval. *Carpenter* defined the term that way, in a parenthetical, and then refused to decide the question. "Our decision today is a narrow one," the Court wrote. "We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)."[17] What the Court *did* decide is the piece prosecutors now treat as the baseline: acquiring historical cell-site records that reconstruct a person's movements is a search, and the government must generally get a warrant. That is why a line prosecutor who wants seven days of one suspect's CSLI does not send a polite letter to Verizon. She writes an affidavit.

The dump is the same tool aimed at the crowd. Instead of "give us this phone's history," the government says "give us everyone who was here." The innocent are in the file because they drove past a robbery, sat in a waiting room, or used the tower that also served the crime. Justice Gorsuch, dissenting in *Carpenter*, asked the question the reservation left open: why isn't a tower dump "the paradigmatic example of 'too permeating police surveillance'"? On what basis, he asked, does mass collection of everyone's data survive a test that seven days of one person's data fails?[18] That is a dissent, not a holding. It is also the right question.

After *Carpenter*, many prosecutors stopped pretending a 2703(d) order was enough and started asking magistrates for warrants before they pulled a dump. That practice is the conservative reading of *Carpenter*. It was not, for years, a single nationwide holding that every dump requires a warrant. The Seventh Circuit said so in 2019. In *United States v. Adkinson*, 916 F.3d 605 (7th Cir. 2019), T-Mobile itself ran dumps of phones near the first two robbed stores; the government used the hits. The court said *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies)) because the Supreme Court declined to rule that these dumps were searches requiring warrants."[19] So the popular claim—that the government cannot get a tower dump without a warrant—was how a careful prosecutor behaved. It was not a sentence you could write as if the Supreme Court had already written it.

The Court has now written the next sentence. The next generation of the dump is the geofence: a reverse-location warrant that tells Google to search Location History for every phone that reported itself inside a drawn box at a drawn time. In *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024), the Fifth Circuit held that "the use of geofence warrants—at least as described herein—is unconstitutional under the Fourth Amendment," and, in closing, that "geofence warrants are modern-day general warrants and are unconstitutional." The convictions stood anyway, under the good-faith exception.[20] A Fourth Circuit panel had gone the other way on a two-hour Google pull; that panel opinion was vacated. The en banc court affirmed in a one-line per curiam and split on whether a search even occurred. The Supreme Court took the case.

On June 29, 2026, in *Chatrie v. United States*, 609 U.S. ___ (2026) (No. 25-112), the Court held that the police conducted a Fourth Amendment search when they acquired Chatrie's location data from Google. Justice Kagan wrote for five Justices; Justice Gorsuch concurred in the judgment. "An individual has a reasonable expectation of privacy in records about his cell phone's location," the Court said, "and police intrude on that constitutionally protected interest when they

demand the information—even though for only a limited time, and from a third-party tech company." It does not matter, the Court said, "if the time period scrutinized was only two hours." Nor does it matter "that the materials obtained were handed over by a third-party tech company." When the government accesses historical cell-phone location information—"Location History as much as CSLI"—it "conducts a search under the Fourth Amendment." The Court left for remand whether the particular multi-step geofence warrant was reasonable—whether it had probable cause and particularity at each step—and it did not decide whether the evidence would be suppressed.[21]

That is the phone holding. A Flock network is the car version of the same architecture, with the warrant application torn off.

The government does not have to go to AT&T and ask for the dump. Flock has already taken it. Every car that passed the camera is in a searchable file for the retention window—often thirty days—by plate, time, place, and "vehicle fingerprint." An officer who wants to know who was on a block last Tuesday, or where a plate has been this month, types a query. No magistrate. No particularity. No minimization. The "tower" is a pole on a city right-of-way. The "carrier" is a private company that sells the dump as a subscription. The "interval" is always on.

That is not *Adkinson*'s one store at one time. It is not two hours of one Google account obtained after a judge was asked. It is *Carpenter*'s duration—days of movement, stored in advance, about everyone—run through a reverse-location design, multiplied across a metro area and, through sharing defaults, across a country. *Chatrie* said two hours from a third party is already a search. A thirty-day Flock query is that search with more time and no warrant. *Knotts* reserved "dragnet-type" law enforcement practices for another day. This is that day, sold as a camera.

Even a court that blessed a thin ALPR deployment said the mosaic can turn into a search when the network gets thick enough. In *Commonwealth v. McCarthy*, 484 Mass. 493 (2020), the Massachusetts Supreme Judicial Court reviewed four readers on the two Cape Cod bridges and concluded that limited deployment was not a search on those facts. The same decision, as quoted in the Commonwealth's official digital-evidence guide, warned that with enough cameras in enough locations, historic ALPR data would invade a reasonable expectation of privacy and constitute a search.[22] A national Flock network is that thicker system. It is a standing tower dump of cars.

The advocacy in this essay is therefore specific. A live glance at a plate in front of an officer can stay a notepad. A historical Flock query that reconstructs who passed a place, or where a car has been over days, is a tower dump—the car-side twin of what *Chatrie* held: accessing historical location data from a third party, even for two hours, is a search. After *Carpenter* and *Chatrie*, a dump of that scale should require a warrant, probable cause, particularity, and a protocol that deletes the innocent. The government would not—or should not—get the phone version of that file by sending a detective a login. It should not get the car version that way either. The only reason the car version looks easier is that the dump was built before the crime and branded as a camera.

V. The statutory map is a patchwork with a hole in the middle

If the Fourth Amendment is late, statutes are uneven.

Illinois's Biometric Information Privacy Act is the most serious American biometric statute, and it is the wrong shape for this problem. It requires private entities to obtain informed written consent before collecting "biometric identifiers," a defined list that includes retina and iris scans, fingerprints, voiceprints, and scans of hand or face geometry. Face-geometry templates used for recognition are in. A raw photograph, without more, is generally out. Gait is not named. Emotion scores are not named. License plates are not biometrics. And BIPA's definition of "private entity" does not include a State or local government agency.[14] The statute that actually produces verdicts against Facebook and factory time-clocks does not, by its terms, regulate the police camera.

Texas, Washington, and a handful of other States have biometric or health-data laws of varying teeth. There is no comprehensive federal privacy statute. There is no comprehensive federal rule that says a city may not fuse ALPR, face, gait, and broker location into one query. Retention is a contract term. Sharing with a neighboring county, or with a federal partner, is often an admin setting. The

European AI Act treats untargeted scraping of faces, certain real-time remote biometric identification in public, and workplace emotion recognition as prohibited or tightly confined practices. American cities are still arguing about whether a plate camera is "Orwellian."

That mismatch is why the Flock fight feels loud and changes little. A city can ban one vendor and leave Clearview, Axon, Fusus, Amazon Ring, school-bus cameras, doorbell networks, and data brokers running. A vendor can truthfully say "we do not do facial recognition" while selling a PTZ camera that follows people and a network that other software can label later. An officer can stay inside the four corners of a use policy and still assemble, from lawful fragments, the dossier *Carpenter* described.

VI. Fusion is the search

The legal error is atomization. The practical error is the same error with a product manager's vocabulary.

Call the plate query Tool A. Call the face search Tool B. Call the phone-broker replay Tool C. Call the body and affect model Tool D. Call last month's Google ads segment Tool E. No one tool looks like an ankle monitor. The join is the ankle monitor.

That is not a metaphor borrowed from science fiction. It is *Carpenter*'s facts with more sensors. Historical CSLI was powerful because it was "detailed, encyclopedic, and effortlessly compiled," retrospective, and collected about everyone in advance.[15] A national vehicle network is detailed, encyclopedic, and effortlessly compiled. A face database of tens of billions of images is the name layer. Broker pings are the indoor layer—the part *Carpenter* said a car does not capture and a phone does. Gait and body-change models are the medical layer. Affect models are the mental-state layer. Marketing and search data are the intent layer. Once those layers share an identifier—plate, phone ad-ID, face template, home address—the person is reidentified even if every vendor swore the feed was anonymous.

The "soon" in this story is shorter than the political cycle. Weight-change and limp detection are not waiting for a new Constitution. They are waiting for a procurement. Emotion scores are already in retail and hiring products. The only question is whether they are bolted onto the same public-safety platform that already logs the car. If that bolt-on is allowed because each piece was approved separately, the Flock hearings will read, in ten years, like an argument about which brand of lock to put on an open house.

There is also a First Amendment problem that Fourth Amendment doctrine keeps treating as someone else's work. Sotomayor's point about chill is the point. People who know that a trip to a church, a union hall, a campaign office, a clinic, or a lawyer's building is stored, named, and scored will go less often, or by stranger routes, or not at all. That is not a privacy injury in the consumer-statute sense. It is a change in the relationship between citizen and government. She quoted the warning that cheap, discretionary tracking may "alter the relationship between citizen and government in a way that is inimical to democratic society." She also recalled the Fourth Amendment's aim to prevent "a too permeating police surveillance."[16] A network that already logs the innocent in order to be ready for the guilty is that surveillance. Adding a face and a mood score does not make it more "conventional." It makes the loophole unlivable.

This fusion argument is advocacy, not a holding. *Carpenter* said it was deciding a "narrow" question about carrier CSLI. *Jones* decided a trespass. *Beautiful Struggle* decided a particular aerial program. No court has yet held that an ALPR network plus a face search plus a broker file is one Fourth Amendment event. That is the gap. It is also the point.

VII. What would a serious response look like?

Not another press release that "Flock does not use facial recognition."

A serious response treats the mosaic as the thing to regulate.

Warrants for movement reconstruction—and for the dump. A live glance at a plate in the moment—an officer checking a car in front of him—can remain a notepad. A historical query that reconstructs where a car, a face, or a phone has been over days should be treated as *Carpenter*. A query that asks who was at a place in a window of time should be treated as a tower dump of that scale: a warrant, probable cause, particularity, and a minimization protocol that deletes the uninvolved.

"I am curious" and "pattern of life" are not enough. The government already pretends this is the rule for phones. It should be the rule for cars. The Fourth Circuit's Baltimore analysis is the closest published model: accessing the *dataset* is the search, not the flight of the plane.

No government remote biometrics in public without a statute that says so out loud. Face, gait, voice, and iris matching against a civilian population are not "security cameras." If a legislature wants them, it should have to write the program, the watchlist rules, the accuracy thresholds, the audit, and the sunset. Silence should not be permission.

Ban government affect inference. Scoring whether someone looks happy, sad, or "concerned" is too unreliable and too intimate to be a police field. Europe already treated workplace and school versions as unacceptable. An American city should not discover the same thing after a wrongful stop.

Close the government hole in biometric statutes. A law that binds Facebook and exempts the police department is a consumer statute, not a surveillance statute. If BIPA's list is the political starting point, gait, voice in public, and derived body metrics belong on it—and the government belongs in the covered class, with a suppression remedy, not only a damages action against companies.

Regulate the join, not the vendor. Procurement rules should forbid fusing ALPR, face, broker location, and commercial dossiers in one interface unless each query is logged, warranted where *Carpenter* would require it, and technically incapable of silent secondary use. "The other company did the face search" is not a constitutional fact.

Warrants for commercial location and search dossiers. If the government generally cannot get seven days of CSLI from a carrier without a warrant, it should not be able to buy thirty days of app pings from a broker, or a person's search history from an advertiser, by purchase order. The third-party doctrine cannot remain a vending machine.

Retention measured in days, not product defaults. Thirty days of every car in a city is a dossier. Indefinite video is a dossier. Broker histories that go back years are a dossier. Default deletion, no quiet "investigative exception" that swallows the rule, and criminal liability for stalking-by-query are the minimum.

Honesty in the municipal contract. If a Condor follows pedestrians, the contract should not say the system "does not track people." If federal partners can be fed through a local login, the contract should not say the city "does not share with ICE" unless the technical path is actually closed. The current vocabulary is a way to win a council vote, not a way to describe the system.

None of that denies that cameras solve crimes. *Carpenter* did not deny that phones solve crimes. It said the tool was too powerful to run on a relevance standard. The same is true here. Public safety is a real interest. It is not an interest that requires a pre-built, named, medically inferred, commercially enriched file on everyone who bought gas.

VIII. The plate is the decoy

People are right to be upset about Flock cameras. They are the visible edge of a system that logs the innocent so that someone, later, can rewind the city. They have already been misused. They already travel across agencies farther than the town that paid for the pole. They already sit next to video products that follow walkers while the marketing page talks about cars.

They are still the decoy.

Facial recognition is already in the toolkit. Gait and body-change inference are already in the lab and the vendor catalog. Affect scoring is already a commercial feature—prohibited as an AI practice in European workplaces and schools, and available to an American integrator. The phone in the cupholder has already told a broker where the driver sleeps. Google already knows what the driver feared at midnight. The only unfinished project is a single pane of glass that ties the plate to the face to the limp to the mood to the query history.

Online, that project is done. In physical space it is being built in the name of stolen catalytic converters, and it will not stop at converters. If the law keeps asking whether a particular camera "is facial recognition," it will keep answering the wrong question until there is nothing left to protect. The right question is the one Justice Sotomayor asked in *Jones*, and that *Carpenter* and the Fourth Circuit answered for movement data: whether

people retain a reasonable expectation of privacy in the *whole* of their physical movements when the government, or anyone the government can buy from, can reconstruct those movements from public fragments.

They do. Or they did. The cameras are how we find out which.

Notes

[1] Flock Safety, *Flock Updates Privacy, Accountability, Security, and Transparency Safeguards* (Aug. 13, 2026), https://www.flocksafety.com/blog/flock-guardrails-address-lpr-privacy-concerns-and-police-transparency (retrieved Aug. 28, 2026); see also CNN, *Flock rolls out new police auditing and accountability controls* (Aug. 13, 2026).

[1a] See InvestigateTV, *supra* note 3 (federal partners and local logins); Flock's public statements have denied a direct ICE contract while describing agency-controlled sharing. The access path is a local-login / sharing question, not a claimed secret Flock–ICE product.

[2] Flock Safety, Trust / FAQ ("Do Flock cameras use facial recognition?"), https://www.flocksafety.com/trust (quoted language as published Aug. 28, 2026).

[3] InvestigateTV, *Flock says its cameras don't track people, training videos say otherwise* (June 15, 2026), https://www.investigatetv.com/2026/06/15/flock-says-its-cameras-dont-track-people-its-own-training-videos-say-otherwise/ (retrieved Aug. 28, 2026).

[4] Regulation (EU) 2024/1689 (Artificial Intelligence Act), Art. 5 (prohibited practices, including emotion recognition in workplaces and education, with limited exceptions). Confirm current article text before relying on a specific subsection number.

[5] *Riley v. California*, 573 U.S. 373, 134 S. Ct. 2473 (2014) (Roberts, C.J.) (slip op. at 17) ("minicomputers"; "They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

[6] *United States v. Knotts*, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). The Court reserved "dragnet-type" practices for another day. *Id.* at 283–84. *Smith v. Maryland*, 442 U.S. 735 (1979) (pen register); *United States v. Miller*, 425 U.S. 435 (1976) (bank records).

[7] *United States v. Jones*, 565 U.S. 400, 404 (2012) (Scalia, J.) (vehicle is an "effect"; installation and use of the GPS device constituted a search).

[8] *Id.* at 415–16 (Sotomayor, J., concurring). The inner quotation "limited police resources and community hostility" is from *Illinois v. Lidster*, 540 U.S. 419, 426 (2004).

[9] *Id.* at 416 (Sotomayor, J., concurring). The "reasonably expect" sentence is framed as the question she "would ask," not as the Court's holding.

[10] *Carpenter v. United States*, 585 U.S. 296 (2018) (Roberts, C.J.) (official slip op., No. 16-402). Seven-day holding: slip op. at 11 n.3. Warrant "generally" required, with exigency reserved: slip op. at 18, 21–22. The first MetroPCS order sought a longer window; the records produced spanned 127 days.

[11] *Id.* (decision described as "a narrow one"; conventional tools including "security cameras" reserved) (slip op. at 17–18).

[12] *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021) (en banc) (Gregory, C.J.) (preliminary-injunction appeal; "likely to succeed on the merits"; three dissenting opinions). Official CA4 PDF, No. 20-1495, https://www.ca4.uscourts.gov/opinions/201495A.P.pdf.

[13] *Kyllo v. United States*, 533 U.S. 27, 34, 40 (2001).

[14] 740 ILCS 14/10 (definitions of "biometric identifier" and "private entity"); 740 ILCS 14/15(b) (informed written consent). Confirm current code text.

[15] *Carpenter*, 585 U.S. 296 (CSLI described as "detailed, encyclopedic, and effortlessly compiled").

[16] *Jones*, 565 U.S. at 416–17 (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), and *United States v. Di Re*, 332 U.S. 581, 595 (1948)). Both reporter cites verified (CL clusters 215613 and 104490).

[17] *Carpenter*, 585 U.S. 296 (official slip op. at 17–18) ("We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval).").

[18] *Id.* (Gorsuch, J., dissenting) (official slip op. at 11 of the dissent) (asking why a tower dump is not "the paradigmatic example of 'too permeating police surveillance'" and on what basis mass collection survives while seven days of one person's data does not). Dissent, not a holding.

[19] *United States v. Adkinson*, 916 F.3d 605 (7th Cir. 2019) (Barrett, J.) (CL cluster 4590846). The quoted "did not invalidate warrantless tower dumps" sentence is from the Seventh Circuit's discussion of *Carpenter*; the local file is an excerpt from CourtListener `html_with_citations`, not a paginated F.3d print. The dumps covered the first two victim stores.

[20] *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024) (King, J.) (CL cluster 10036119). Opening: "We hold that the use of geofence warrants—at least as described herein—is unconstitutional under the Fourth Amendment." Closing: "We hold that geofence warrants are modern-day general warrants and are unconstitutional under the Fourth Amendment." Good-faith exception preserved the convictions. CourtListener `citing` with overruling / abrogation / vacatur / rehearing terms returned no hits as of August 29, 2026. Not a commercial KeyCite. *Chatrie* did not cite *Smith* and remanded the particularity question.

[21] *Chatrie v. United States*, 609 U.S. ___ (2026) (No. 25-112, slip op. June 29, 2026) (Kagan, J., joined by Roberts, C.J., and Sotomayor, Kavanaugh, and Jackson, JJ.; Gorsuch, J., concurring in the judgment), https://www.supremecourt.gov/opinions/25pdf/25-112_0am4.pdf (CL cluster 10881683). Opening quotation: slip

op. at 2. Closing cluster ("two hours" / third-party company / "Location History as much as CSLI"): slip op. at 29. The Fourth Circuit panel opinion, 107 F.4th 319 (2024), was vacated. The en banc judgment is *United States v. Chatrie*, 136 F.4th 100 (4th Cir. 2025) (en banc) (per curiam), vacated and remanded by the Supreme Court. The Court decided only that acquiring the Location History was a search; it left probable cause, particularity, and the exclusionary-rule question to the Fourth Circuit.

[22] *Commonwealth v. McCarthy*, 484 Mass. 493 (2020) (SJC; CL cluster 4746120). CourtListener citation-lookup 404s on the Massachusetts reporter. This essay does not quote the slip. The four-camera / two-bridge facts and the "enough cameras" warning are taken from the official Massachusetts *Digital Evidence Guide* (mass.gov) summarizing the SJC. Confirm the bound volume before filing-level use.