The Plate Is Not the Person:

What Owner Liability Already Concedes About Automated Vehicle Surveillance

Travis Gilly* August 2026 (v1)

Abstract

A camera at the roadside records a registration plate. A database converts that record into an assertion about where a person has been. Nothing in the pipeline verifies that the person was ever in the vehicle. This article names that conversion silent attribution, names the space it crosses the attribution gap, and argues that American law has already adjudicated both, where no one has looked.

Automated traffic enforcement concedes the premise three times. Illinois supplies defenses when a vehicle or its plates were stolen and therefore "not under the control of or in the possession of the owner," language a legislature writes only when it knows the owner is frequently not the driver. The Seventh Circuit upheld owner liability in *Idris v. City of Chicago* on the reasoning that a camera reliably shows which vehicles ran a light but is less likely to show who was driving, leaving a city essentially unable to prove otherwise. And in *Tupper v. City of St. Louis* the Supreme Court of Missouri struck down a camera ordinance for creating a presumption that shifted the burden of persuasion onto the owner to prove he was not the operator.

Plate reader doctrine has developed as though none of that existed. Courts ask whether a plate is exposed to public view and whether accumulated location points reconstruct the whole of a person's movements. Both questions presuppose that the vehicle's movements are the person's, and the leading decisions do not defend that premise because they never reach it. *Kansas v. Glover* authorized the inference for reasonable suspicion alone, only absent contrary information, and only where an officer looking at the driver can dispel it. Database retrieval removes all three.

The article then tests the justification the networks are sold on. Substituting a plate defeats a reader more cheaply than avoiding one, and it does not produce invisibility. It produces misdirection onto a registered owner who was never present, which the system cannot detect and which the falsely named owner learns by mail.

The contributions are three. It locates a statutory and judicial admission that a plate does not identify a driver, sitting in the jurisdictions that treat plate data as location history. It shows that no stage of retrieval records the moment a vehicle observation becomes a claim about a person. And it identifies the class whose recorded travel is false in its entirety: registered owners who do not drive.

Keywords: Fourth Amendment; surveillance law; license plate readers; silent attribution; attribution gap; mosaic theory; vicarious liability; evidentiary foundation; Flock Safety; nondriving registered owners; traffic camera adjudication; disability and mobility.

*Travis Gilly is Founder and Executive Director of the Real Safety AI Foundation. ORCID: 0009-0007-2954-6313. Correspondence: t.gilly@ai-literacy-labs.org. The author discloses the use of speech-to-text software (Wispr Flow) and Anthropic's Claude as assistive technology for a diagnosed neurodevelopmental condition. All legal analysis, case synthesis, theoretical framing, doctrinal arguments, and conclusions are solely the author's own.

Contents

I. Introduction

Two automated systems read the same registration plate on the same road in the same state. One of them has been told by a federal court of appeals that it cannot identify the driver. The other is treated, without argument, as producing a record of where a person has been.

The first system is automated traffic enforcement. When a camera records a vehicle entering an intersection against a red signal, Illinois law directs the resulting notice to the registered owner and imposes a civil penalty on that person, whether or not the owner was behind the wheel.[1] The Seventh Circuit upheld that architecture in *Idris v. City of Chicago*, and the reason it gave is the subject of this article: "A camera can show reliably which cars and trucks go through red lights but is less likely to show who was driving."[2] Judge Easterbrook continued that a requirement to identify the driver "would make it easy for owners to point the finger at friends or children," and "essentially impossible for the City to prove otherwise."[3] Owner liability exists because the camera cannot see who is driving.

The second system is the automated plate recognition network. The same class of roadside camera reads the same plate, writes the read to a database with a timestamp and a location, and retains it.[4] Courts assessing that system ask whether a motorist has a reasonable expectation of privacy in the exterior of a vehicle,[5] and whether the accumulated reads reconstruct enough of a person's travel to implicate the whole of that person's public movements.[6] Both questions take for granted that the vehicle's movements are the person's

1. 625 Ill. Comp. Stat. 5/11-208.6(j) (imposing civil liability on the vehicle owner absent a uniform traffic citation issued to the driver by a police officer at the time of the violation).

2. *Idris v. City of Chicago*, 552 F.3d 564, 566 (7th Cir. 2009).

3. *Id.*

4. *See United States v. Sturdivant*, 786 F. Supp. 3d 1098, 1117 (N.D. Ohio 2025) (describing the retrospective operation of historical plate reader data and noting that officers may "travel back in time to retrace a [vehicle's] whereabouts, subject only to the retention policies" of vendors such as Flock or of government operators (quoting *Carpenter v. United States*, 585 U.S. 296, 312 (2018))).

5. *See New York v. Class*, 475 U.S. 106, 114 (1986) ("The exterior of a car, of course, is thrust into the public eye, and thus to examine it does not constitute a 'search.' ").

6. *See Commonwealth v. McCarthy*, 484 Mass. 493, 508–09, 142 N.E.3d 1090 (2020) ("With enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes.").

movements. Neither the plain view line nor the aggregation line defends that assumption. They do not reach it.

This article gives the assumption a name and asks what happens when it is examined. Silent attribution is the conversion, occurring somewhere between the camera and the case file, of an observation about an object into an assertion about a human being. The attribution gap is the space that conversion crosses. It is a gap because nothing in the pipeline measures it, marks it, or preserves any record that it was crossed.

The argument proceeds in six steps. Part II establishes the admission. Illinois recognizes the owner-driver divergence twice in statutory text, providing defenses when a vehicle or its plates were stolen or when the vehicle was hijacked, in each case because the vehicle was "not under the control of or in the possession of the owner or lessee at the time of the violation."[7] A legislature does not draft that clause unless it knows the owner is frequently not the operator. Part II also shows what the enforcement regime pays for the fiction it adopts: a civil rather than criminal penalty, a statutorily specified notice, and an election among a court proceeding, a mail contest, and an administrative hearing.[8]

Part II closes with *Tupper v. City of St. Louis*, in which the Supreme Court of Missouri struck down a camera ordinance for creating a presumption that shifted onto the owner the burden of proving he was not the operator.[9] That decision is the nearest any American court has come to the argument advanced here, and the reason it went no further supplies this article's thesis: what made the St. Louis presumption reviewable is that the ordinance stated it.

Part III shows that plate reader doctrine runs the same inference without paying anything for it, and closes with an episode in which the category the doctrine analyzes came apart. Part IV isolates the moment of attribution and shows that no stage of the pipeline records it. Part V tests the justification on which the networks are sold, which is the prevention of serious

7. 625 Ill. Comp. Stat. 5/11-208.6(h)(1), (h)(1.5).

8. *Id.* § 11-208.6(d)(10)(B) (requiring the notice to state that the person may elect to proceed by challenging the charge in court, by mail, or at an administrative hearing).

9. *Tupper v. City of St. Louis*, 468 S.W.3d 360, 364 (Mo. 2015).

crime, and finds that substituting a plate defeats a reader more cheaply than avoiding one, that substitution produces misdirection onto an innocent registered owner rather than invisibility, and that detection of the substitution runs through that owner's mail rather than through the system. Part VI works through the consequences for evidentiary foundation, Fourth Amendment analysis, and procedural due process, identifies the population that absorbs the error without remainder, and measures what the reforms now on offer actually reach. Part VII concludes.

The claim is not that plate readers are useless or that the inference is always wrong. It is narrower and, for that reason, harder to answer. Where American law has confronted the question directly, it has resolved it against the premise that a plate identifies a driver. Where American law has treated plate data as a person's location record, it has never confronted the question at all.

II. The Admission

A. Owner Liability Is a Concession, Not an Assumption

Automated traffic enforcement statutes are unusual among penal and civil penalty regimes in that they name, in text, the person who will be held responsible for conduct that person may not have performed. Illinois provides that unless a police officer issued a uniform traffic citation to the driver at the scene, the owner of the motor vehicle is subject to the civil penalty.[10] Ordinances implementing the statute say the same thing in blunter language. A Missouri municipal provision reviewed by the Missouri Court of Appeals read: "Liability hereunder is based on ownership, without regard to whether the owner was operating the motor vehicle at the time of the violation."[11] A Tennessee court put the point the same way, rejecting an argument that

10. 625 Ill. Comp. Stat. 5/11-208.6(j).

11. *City of Creve Coeur v. Nottebrok*, 356 S.W.3d 252, 259–60 (Mo. Ct. App. 2011) (quoting Ordinance No. 315.140). The decision is cited here for the ordinance text it reproduces and not for its holding, which rests on a points classification later held to conflict with Missouri law. *See City of St. Peters v. Roeder*, 466 S.W.3d 538, 546–47 (Mo. 2015).

the city bore a burden to establish who was in control of the vehicle: the code "makes the owner of the vehicle responsible for a red light violation, regardless of who was driving the vehicle."[12]

The critical move is to read those provisions as evidence rather than as rules. A statute that assigns liability "without regard to" the identity of the operator is a legislative finding that the identity of the operator is unavailable. No drafter writes that clause about a system that produces the driver's name. The provision exists because the record produced by the camera stops at the vehicle.

Illinois makes the finding twice more, and more precisely, in its defense provisions. A court or hearing officer may consider that the vehicle or its plates were stolen before the violation occurred "and not under the control of or in the possession of the owner or lessee at the time of the violation," and separately that the vehicle was hijacked and likewise not under the owner's control or possession.[13] That phrase is the owner-driver divergence stated in statutory language. The legislature knew the owner may not have been in the vehicle, said so, and then made the divergence cognizable in exactly two circumstances, both of which require a criminal act by a third party and a police report.[14]

The structure is worth stating plainly. If a stranger takes the vehicle, the law will hear that the owner was not driving. If a spouse takes the vehicle, the law will not ask. The divergence is a fact of the world in both cases. It is a defense in only one.

B. Idris and the Judicial Finding

Idris converts the legislative premise into a judicial one. The plaintiffs argued that Chicago's ordinance unconstitutionally imposed liability on a vehicle's owner even when the owner was not driving.[15] The Seventh Circuit affirmed dismissal, and the operative passage is an epistemic

12. *City of Knoxville v. Brown*, 284 S.W.3d 330, 338–39 (Tenn. Ct. App. 2008). The court's separate analysis of the Tennessee constitutional limit on fines is not relied on here.

13. 625 Ill. Comp. Stat. 5/11-208.6(h)(1), (h)(1.5). To establish either defense the owner must submit proof that a report was filed with a law enforcement agency. *Id.* § 11-208.6(i).

14. *Id.* § 11-208.6(i).

15. *Idris v. City of Chicago*, No. 1:06-cv-06085 (N.D. Ill. Jan. 16, 2008), *aff'd*, 552 F.3d 564 (7th Cir. 2009).

finding rather than a doctrinal one. Asked whether it is rational to fine the owner rather than the driver, the court answered that it is, because a camera "can show reliably which cars and trucks go through red lights but is less likely to show who was driving," which "would make it easy for owners to point the finger at friends or children" and "essentially impossible for the City to prove otherwise."[16]

Three observations follow. First, the court is describing the evidentiary capacity of roadside camera technology, not the scope of municipal power. Second, the finding is not dictum in any useful sense: the rationality of the ordinance rests on it, and without it the equal protection and due process analysis collapses.[17] Third, the court reached the finding in the Seventh Circuit, which supplies the governing federal law for the Illinois plate reader network discussed in Part III.

Idris placed automated enforcement in a lineage of no-fault penalty regimes, invoking civil forfeiture of a vehicle used in a crime,[18] eviction of a public housing tenant for a guest's conduct,[19] and tax penalties imposed on a taxpayer for an adviser's error.[20] Each of those regimes is candid about what it is doing. Each names a party who did not commit the act and explains why that party should bear the cost anyway. The candor is the point. A no-fault regime that announces itself invites the objection that it is a no-fault regime.

The court also relied on the modest stakes. Substantive due process requires a fundamental liberty interest, and "[t]he interest at stake is a $90 fine for a traffic infraction."[21] That reasoning transfers poorly. A ninety dollar civil penalty and a retained record spanning years of a person's movements are not the same interest, and the second was not before the court.

16. *Idris*, 552 F.3d at 566.

17. *See id.* (grounding the rational-basis conclusion on the reduced cost of enforcement achievable "only if the owner is held responsible").

18. *Bennis v. Michigan*, 516 U.S. 442 (1996), *cited in Idris*, 552 F.3d at 566.

19. *Dep't of Hous. & Urban Dev. v. Rucker*, 535 U.S. 125 (2002), *cited in Idris*, 552 F.3d at 566.

20. *United States v. Boyle*, 469 U.S. 241 (1985), *cited in Idris*, 552 F.3d at 566.

21. *Idris*, 552 F.3d at 566 (citing *Washington v. Glucksberg*, 521 U.S. 702, 719–22 (1997)).

C. What the Regime Pays for the Fiction

Automated traffic enforcement buys its attribution with procedure. The penalty is civil rather than criminal.[22] The notice must contain statutorily specified contents, including a statement that the recipient may elect to proceed by challenging the charge in court, by mail, or at an administrative hearing.[23] Recorded images are confidential and available only to the alleged violator and to governmental and law enforcement agencies for enumerated purposes.[24] A hearing officer may consider enumerated defenses and "any other evidence or issues provided by municipal or county ordinance."[25]

None of this is generous. Courts have repeatedly held that the process afforded is constitutionally adequate,[26] and the Seventh Circuit has treated the administrative apparatus as functionally identical to the parking ticket system it approved in *Van Harken*.[27] The point is not that the procedure is robust. The point is that it exists, that the legislature enacted it alongside the attribution, and that it is the measure of what a legislature thought an admitted attribution error was worth.

Not every judge has been satisfied. Dissenting in *City of St. Peters v. Roeder*, Judge Draper objected that camera enforcement effectively presumes "that the registered owner committed the violation," compelling the owner "to put forth evidence that the vehicle has been sold or stolen, or the owner must appear in court to identify another driver," and concluded that "this rebuttable presumption is impermissible."[28] Judge Stith, concurring in part, put the

22. 625 Ill. Comp. Stat. 5/11-208.6(j).

23. *Id.* § 11-208.6(d)(10)(B).

24. *Id.* § 11-208.6(g).

25. *Id.* § 11-208.6(h)(3).

26. *See City of Sioux City v. Jacobsma*, 862 N.W.2d 335, 344–46 (Iowa 2015) (surveying decisions upholding owner liability against due process challenge); *Krieger v. City of Rochester*, 42 Misc. 3d 753, 771–72 (N.Y. Sup. Ct. 2013) (collecting federal decisions rejecting due process challenges to camera enforcement programs).

27. *Idris*, 552 F.3d at 567 (citing *Van Harken v. City of Chicago*, 103 F.3d 1346 (7th Cir. 1997)).

28. *City of St. Peters v. Roeder*, 466 S.W.3d 538, 552–53 (Mo. 2015) (Draper, J., dissenting).

objection in terms this article adopts: the ordinance "create[s] the impression, if not the reality, that it is [the citizen's] burden to prove that they were not the driver."[29]

The same court had already acted on the point. In *Tupper v. City of St. Louis*, decided the same day, the Supreme Court of Missouri held a camera ordinance "constitutionally invalid because it creates a rebuttable presumption that shifts the burden of persuasion onto the defendant to prove that the defendant was not operating the motor vehicle at the time of the violation."[30] The court grounded the holding in the rule that a mandatory rebuttable presumption shifting the burden of persuasion on an element offends due process.[31]

Tupper is the closest any American court has come to the argument advanced here, and the distance it did not travel is the subject of the rest of this article. What made the St. Louis presumption reviewable is that the ordinance said it. A court could read the provision, identify the inference, locate the burden, and strike it. The plate reader network runs the identical inference and writes it down nowhere, which is why no court has struck it. All of these objections were directed at a fine accompanied by a hearing. None has been directed at a location database accompanied by nothing.

III. The Same Inference, Unbounded

A. The Plain View Line

Plate reader doctrine begins from two propositions that are settled and, standing alone, correct. A license plate is required by law to be displayed in a place ordinarily visible from outside the

29. *Id.* at 551 (Stith, J., concurring in part and in result).

30. *Tupper v. City of St. Louis*, 468 S.W.3d 360, 364 (Mo. 2015).

31. *Id.* at 375–76 (discussing *Sandstrom v. Montana*, 442 U.S. 510, 517–18 (1979)).

vehicle, so there is no reasonable expectation of privacy in it.[32] And a person traveling on public thoroughfares has no reasonable expectation of privacy in movement from one place to another.[33]

From those premises, courts have concluded with near uniformity that operating a plate reader network is not a Fourth Amendment search. The Northern District of Illinois so held in *Scholl v. Illinois State Police*, sustaining the state's expressway camera program on the reasoning that motorists have a diminished expectation of privacy in the exterior of a vehicle and in public movement.[34] The Northern District of Ohio reached the same result on database queries in *Sturdivant*, holding that a defendant "has no reasonable expectation of privacy in the appearance of his vehicle or in his license plate number," so that querying a database containing that information is not a search.[35] A district court in Pennsylvania summarized the field earlier this year: many courts have found that maintaining a plate reader system is not a search because individuals possess no expectation of privacy in their plates and because locating a vehicle does not involve the monitoring at issue in cell-site cases.[36]

Read carefully, none of those holdings is about a person. *Class* concerns the exterior of an automobile.[37] *Cardwell* concerns a car's capacity to escape public scrutiny.[38] *Sturdivant* speaks of the appearance of the defendant's vehicle and his plate number.[39] The doctrine is about objects, and it is sound about objects. The slippage occurs when a conclusion about the observability of an object is carried forward as a conclusion about the surveillance of a person.

---

32. *New York v. Class*, 475 U.S. 106, 114 (1986); *see also Commonwealth v. Long*, 152 N.E.3d 725, 731 (Mass. 2020) ("[T]here is no expectation of privacy in a license plate number, which is required by law to be displayed conspicuously on the exterior of a vehicle.").

33. *United States v. Knotts*, 460 U.S. 276, 281–82 (1983); *see also Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) ("A car has little capacity for escaping public scrutiny.").

34. *Scholl v. Ill. State Police*, 776 F. Supp. 3d 701, 719 (N.D. Ill. 2025) (concluding that "Illinois's installation and use of the ALPR system is not a 'search' subject to Fourth Amendment scrutiny").

35. *Sturdivant*, 786 F. Supp. 3d at 1113.

36. *Heller v. Brookhaven Borough*, No. 2:25-cv-05550, slip op. at 14–15 (E.D. Pa. Feb. 11, 2026).

37. *Class*, 475 U.S. at 114.

38. *Cardwell*, 417 U.S. at 590.

39. *Sturdivant*, 786 F. Supp. 3d at 1113.

B. The Aggregation Line

The second line of authority accepts that individually public observations may in the aggregate produce something the Fourth Amendment protects. The reasoning descends from Justice Sotomayor's concurrence in *United States v. Jones*, asking 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."[40] It is generally called the mosaic theory, and it has generated a substantial and largely skeptical literature.[41]

McCarthy is the leading application to plate readers. The Supreme Judicial Court of Massachusetts held that a defendant has a constitutionally protected expectation of privacy in the whole of his public movements, that the interest could be implicated by widespread plate reader deployment, but that four cameras at two bridge locations did not invade it.[42] The court was explicit about the prospective rule: "With enough cameras in enough locations," historic plate reader data "would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes."[43] Massachusetts has since applied that line, sustaining a limited inquiry that "did not reveal whether the defendant's entry to and exit from the relevant region was an aberration or a pattern."[44] The Seventh Circuit has considered the theory in the pole camera setting and declined to adopt it, observing that the Supreme Court has not required lower courts to apply it.[45]

---

40. *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

41. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 313–14 (2012) (identifying the theory and questioning its administrability); *see also* Jace C. Gatewood, *It's Raining Katz and Jones: The Implications of* United States v. Jones*, A Case of Sound and Fury*, 33 Pace L. Rev. 683 (2013) (arguing that neither *Jones* nor *Katz* adequately protects against nontrespassory accumulation of movement data, including through automatic plate recognition).

42. *McCarthy*, 484 Mass. at 494–95, 142 N.E.3d 1090.

43. *Id.* at 508–09.

44. *Commonwealth v. Govan*, 259 N.E.3d 370, 383 (Mass. 2025) (discussing *McCarthy*, 484 Mass. at 508–09).

45. *United States v. Tuggle*, 4 F.4th 505, 517–19 (7th Cir. 2021).

The aggregation line is more protective than the plain view line, and it fails the same way. Its unit of analysis is a person's movements. Its evidence is a vehicle's movements. *McCarthy*'s own reasoning treats the vehicle's travel as the defendant's travel throughout, without a step that establishes the connection. That is not a criticism of the outcome. It is an observation that the premise was never litigated, which means it was never tested. Part IV takes that observation up as a claim about the field rather than about a single opinion, and offers an account of why the litigation has not occurred.

C. Chatrie and the Premise That Does Not Transfer

The Supreme Court's most recent location decision makes the missing step visible by contrast. In *Chatrie v. United States*, the Court held that officers conduct a Fourth Amendment search when they obtain a person's Location History from a third party, because an individual "has a reasonable expectation of privacy in records about his cell phone's location."[46] The Court rejected the argument that two hours of data was too brief to matter, declining to recognize any "Constitution-free zone" for short-term digital location tracking and invoking *Jones*'s observation that even short-term monitoring can supply "a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations."[47] It held the third-party doctrine inapplicable because Location History is not "truly shared" in any ordinary sense and is instead "the automatic price of conventional cell phone usage."[48]

The reasoning is powerful, and every step of it depends on a fact about the device. *Carpenter* rested on the proposition that a cell phone is a pervasive and insistent part of daily life carried by its user.[49] *Riley* had earlier described the modern phone in similar terms.[50] The location record stands in for the person because the object stands in for the person. Scholarship in

46. *Chatrie v. United States*, 609 U.S. ___, No. 25-112, slip op. at 2 (2026).
47. *Id.* at 19–20 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).
48. *Id.* at 25–26 (quoting *Carpenter*, 585 U.S. at 315).
49. *Carpenter*, 585 U.S. at 311, 315.
50. *Riley v. California*, 573 U.S. 373, 385 (2014).

this area has organized itself around the same premise, asking how the Fourth Amendment should treat data radiating from devices carried on and about the body.[51]

A vehicle is a different kind of object, and the difference is not a matter of degree. A household car is shared, lent, borrowed, driven by adolescents, driven by a spouse, held in one name for reasons of credit or insurance, and titled to a person who may never operate it. The Illinois statute assumes as much on its face when it contemplates that a vehicle may be "not under the control of or in the possession of the owner or lessee at the time of the violation."[52] Applying an inference calibrated to an object carried on the body to an object parked in a driveway is not an extension of *Carpenter*. It is a substitution of one premise for another without a supporting argument.

D. Glover and the Conditions the Database Removes

The strongest authority for the inference from plate to driver is *Kansas v. Glover*, and read closely it is the best support for the argument advanced here. An officer ran a plate, learned the registered owner's license was revoked, and stopped the vehicle on the assumption that the owner was driving.[53] The Court held that "[w]hen the officer lacks information negating an inference that the owner is driving the vehicle," the resulting investigative stop is reasonable.[54]

Three limits are built into that sentence and each is doing work. First, the inference was approved for reasonable suspicion, the lowest individualized standard in Fourth Amendment law, resting on "commonsense judgments and inferences about human behavior" and on probabilities rather than on proof.[55] Second, the inference is conditional on the absence of contrary information. Third, and most important here, the Court explained how the inference gets

---

51. *See* Andrew Guthrie Ferguson, *The Smart Fourth Amendment*, 102 Cornell L. Rev. 547, 550–53 (2017) (describing sensor data from devices on or about the body and proposing informational curtilage); Shaun B. Spencer, *Predictive Surveillance and the Threat to Fourth Amendment Jurisprudence* (2018) (unpublished manuscript) (analyzing accommodation of aggregated behavioral prediction within existing doctrine).

52. 625 Ill. Comp. Stat. 5/11-208.6(h)(1).

53. *Kansas v. Glover*, 589 U.S. 376, 378–79 (2020).

54. *Id.* at 380.

55. *Id.* at 380–81 (quoting *Illinois v. Wardlow*, 528 U.S. 119, 125 (2000)); *id.* at 382 ("officers, like jurors, may rely on probabilities in the reasonable suspicion context").

dispelled: "if an officer knows that the registered owner of the vehicle is in his mid-sixties but observes that the driver is in her mid-twenties, then the totality of the circumstances would not raise a suspicion that the particular individual being stopped is engaged in wrongdoing."[56]

That example describes an officer looking at a driver. The whole structure holds together because an officer at the roadside occupies a position from which the inference can fail in real time. Justice Kagan, concurring, emphasized how narrow the ground was, tying it to the specific inference that a person who has already flouted driving restrictions will drive again.[57] Justice Sotomayor, dissenting, objected that the majority had substituted lay intuition for the reasonable officer's experience and shifted the burden accordingly.[58]

Retrieval from a plate reader database removes every condition *Glover* relied on. The query is retrospective, so no one is positioned to observe the driver at the moment of the read.[59] The capture is indiscriminate, sweeping every passing vehicle rather than one under momentary scrutiny.[60] And the resulting record preserves no field in which the absence of driver observation could be noted, so the inference cannot fail later either. *Glover* authorized a fragile, correctable guess made by a person who was watching. The database inherits the guess and discards the correction.

E. The Category the Doctrine Analyzes

Every decision surveyed in this Part evaluates a device that reads registration plates, and reasons from the legal status of the plate to the constitutional status of the network. That reasoning is only as sound as its description of the device.

In December 2025 the description was tested by accident. Two researchers found sixty-seven cameras belonging to the dominant vendor streaming to the open internet without

56. *Id.* at 385 (quoting *United States v. Cortez*, 449 U.S. 411, 418 (1981)) (internal quotation marks omitted).

57. *Id.* at 387–88 (Kagan, J., concurring).

58. *Id.* at 392–93 (Sotomayor, J., dissenting).

59. *Sturdivant*, 786 F. Supp. 3d at 1117 (noting that historical plate reader data operates retrospectively and that "law enforcement does not need any advance suspicion to track a vehicle").

60. *Id.*

authentication, exposing live feeds, up to thirty days of archived video, and the administrative interfaces, which search engines had indexed.[61] A reporter stood at an intersection in Bakersfield, California and watched himself on the exposed feed while colleagues viewed the same stream from hundreds of miles away.[62]

The exposed devices were not plate readers. They belonged to the vendor's Condor line, which pans, tilts, zooms, and applies machine classification to identify and follow people, vehicles, and other objects, and which, according to the researcher who located them, mostly did not include plate reading at all unless purchased as an add-on carrying an annual fee.[63] The exposed feeds covered parking lots, bike paths, public trails, residential areas, and a playground, and one camera zoomed automatically on a man rollerblading along a public greenway.[64]

The doctrinal consequence is narrow and it is not cosmetic. The plain view line rests on the premise that the observed object is an identifier the law requires to be displayed on a vehicle's exterior.[65] That premise is accurate as applied to a plate reader. It has no application to a camera following a pedestrian on a footpath. A court reasoning from *Class* to the conclusion that a municipal camera network is not a search is reasoning about a category that no longer describes what the municipality purchased, because one vendor sells both classes of device under one relationship and frequently under one contract.

The episode also supplies an unplanned test of the assumptions these decisions make about retention and access. *McCarthy* treated a one-year retention policy as a fact about the

---

61. Jason Koebler, *Flock Exposed Its AI-Powered Cameras to the Internet. We Tracked Ourselves*, 404 Media (Dec. 22, 2025), https://www.404media.co/flock-exposed-its-ai-powered-cameras-to-the-internet-we-tracked-ourselves/ (last visited Aug. 21, 2026); *see also* Jon Gaines, *Finding 67 Flock Safety Live PTZ Camera and LPR Feeds and Debug Web Interfaces Accidentally Exposed Without Authentication to the Internet* (Jan. 9, 2026), https://gainsec.com/2026/01/09/bird-hunting-season-finding-67-live-camera-feeds-and-debug-web-interfaces-accidentally-exposed-by-f (last visited Aug. 21, 2026).

62. Koebler, *supra* note 61.

63. *Douglas County's Flock Camera Compromised as Company Leaves It Exposed on Internet*, 9News (Dec. 23, 2025), https://www.9news.com/article/news/local/colorado-news/douglas-county-flock-cam-compromised-leaves-camera-exposed/73-b (last visited Aug. 21, 2026) (reporting that Condor cameras differ from the vendor's solar-powered plate readers and that most Condor units examined lacked plate reading absent a paid add-on).

64. *Id.*; Koebler, *supra* note 61.

65. *Class*, 475 U.S. at 114.

system,[66] and *Sturdivant* described retrospective retrieval as "subject only to the retention policies" of the vendor or the government operator.[67] For thirty days of footage on sixty-seven devices, the operative retention policy was whoever found the link. The vendor characterized the exposure as a limited misconfiguration affecting a small number of devices.[68] One month earlier, a United States Senator had asked the Federal Trade Commission to investigate the same company's failure to require multi-factor authentication on law enforcement accounts, noting that its data "can reveal Americans' movements over time, including trips to doctors and therapists, support group meetings for alcohol or drug addiction, as well as places of worship and protests."[69]

IV. Silent Attribution

A. Locating the Conversion

It is worth being precise about where the error is manufactured, because precision here identifies an act and an actor.

The capture event does not name anyone. A plate reader records an alphanumeric string, a timestamp, a location, and an image of the vehicle. Courts describing the technology consistently describe it in those terms, and one has observed that the photographic character of the output supplies "richer visual information about the car and its surroundings" than cell-site data does.[70] Nothing in that record is a person.

The conversion happens later, when someone resolves the plate against a registration database and treats the result as the identity of a traveler. That step is a discrete act performed by

66. *McCarthy*, 484 Mass. at 508–09, 142 N.E.3d 1090.

67. *Sturdivant*, 786 F. Supp. 3d at 1117 (quoting *Carpenter*, 585 U.S. at 312).

68. *Flock Camera Captured Kids on a Playground. A Security Failure Exposed Them Online*, Straight Arrow News (Dec. 22, 2025), https://san.com/cc/flock-camera-captured-kids-on-a-playground-a-security-failure-exposed-them-online/ (last visited Aug. 21, 2026).

69. Letter from Sen. Ron Wyden to Andrew N. Ferguson, Chairman, Fed. Trade Comm'n (Nov. 3, 2025), https://www.wyden.senate.gov/imo/media/doc/wyden_letter_to_ftc_on_flockpdf.pdf (last visited Aug. 21, 2026).

70. *Sturdivant*, 786 F. Supp. 3d at 1117.

an identifiable actor at an identifiable time. It is the step at which a fact about an object becomes an assertion about a human being.

The pipeline preserves no trace of the step. The read is stored as data. The registration lookup returns a name. The name enters an affidavit, a report, or an alert. At no point does the record carry a field reading "driver not observed," because no schema contains one. A downstream reader of the file, acting in complete good faith, receives an assertion that a person was at a place and has no means within the record of learning that the assertion is an inference.

That is why silent attribution is the right name for it. The conversion is not concealed. It is simply not written down.

B. The Courts Have Not Reached It

Part III recorded, as an observation about *McCarthy*, that the premise was never litigated there. Stated in that form it is a remark about one opinion, and a remark about one opinion is easy to absorb: courts pass over incidental questions all the time, and nothing follows from a single instance. The claim is worth defending in its stronger form. The premise has not been litigated anywhere, and its survival is a product of who is positioned to raise it rather than of any court having considered and accepted it. What follows is the argument for that proposition.

An objection presents itself immediately: if the premise were unsound, litigants would have raised it and courts would have resolved it. The record does not support that inference. The two most substantial plate reader decisions in the field both stop short of the question.

McCarthy treats the vehicle's movements as a proxy for the defendant's movements without a technical distinction between them, and the opinion contains no analysis of who was driving on the occasions the cameras recorded.[71] *Scholl* sustains the Illinois program on plain view grounds and on standing, and the distinction between driver and owner appears nowhere

71. *McCarthy*, 484 Mass. at 494–95, 508–09, 142 N.E.3d 1090. Chief Justice Gants, concurring, would have required agencies to preserve every search query for historical location data so that a reviewing court could assess the extent of the mosaic actually assembled. *Id.* at 517–19 (Gants, C.J., concurring).

in its reasoning.[72] The Illinois statute governing that program limits camera use to enumerated serious offenses and to highway safety and incident management,[73] which is a substantive limit on purpose and not a limit on attribution.

The reason for the silence is structural rather than accidental. Fourth Amendment plate reader litigation arises almost entirely on motions to suppress brought by criminal defendants, and a defendant who was in fact driving has no incentive to argue that the record fails to establish who was driving. The person with the incentive to raise it is the registered owner who was somewhere else, and that person is not a party, has no notice that a record exists, and under *Scholl*'s standing analysis faces a substantial obstacle even to reaching the merits.[74] The premise survives not because it has been defended but because the only party positioned to contest it is outside the courthouse.

V. The Justification, and the Plate

A. What the Architecture Is Sold to Do

An argument this far along invites the response that the attribution error, whatever its size, is worth tolerating for what the system catches. The response deserves engagement on its own terms, because it is the reason the networks were built and the reason municipalities renew the contracts.

The commercial case is stated plainly. The dominant vendor markets its plate recognition product for recovering stolen vehicles, locating missing people, investigating crimes, and responding to security incidents, and describes its own installation as the nation's largest

72. *Scholl*, 776 F. Supp. 3d at 712–14, 719 (dismissing the database query claim for want of standing where plaintiffs alleged no substantial risk that police would soon retrieve their plate information, and sustaining the collection program on the merits).

73. 605 Ill. Comp. Stat. 140/5, *discussed in Scholl*, 776 F. Supp. 3d at 713.

74. *Scholl*, 776 F. Supp. 3d at 712–14 (finding no substantial risk of imminent retrieval where plaintiffs alleged no conduct that would render their plates relevant to an investigation).

network of such readers.[75] Illinois has written a narrower version of the same justification into statute, authorizing expressway cameras for vehicular hijacking, aggravated vehicular hijacking, terrorism, motor vehicle theft, and forcible felonies, along with highway safety and incident management.[76] That statute is a limit on purpose. It is not a limit on attribution, and the two should not be confused.

B. The Vendor's Own Concession

That justification carries an unstated premise of its own: that the plate identifies the vehicle. The party with the most to lose from questioning that premise has already conceded it in writing.

In a technical post published in February 2026, the vendor acknowledged that "license plates are not always reliable," and that plates "are often swapped, covered, falsified, stolen, altered, misread, or replaced with temporary or paper tags," sometimes simply unreadable.[77] The post exists to market a supplementary vehicle identification capability, and its candor is a function of that purpose. It is nonetheless an admission by the operator of the network that the identifier the network is built on is defeated routinely and by ordinary means.

Illinois prohibits the conduct. No person may display upon a vehicle a registration plate not issued for that vehicle,[78] and it is a violation to display or affix to a vehicle a license plate "not authorized by law for use on such vehicle."[79] The Secretary of State may suspend or revoke a registration when a plate "is knowingly displayed upon a vehicle other than the one for which issued."[80] Prohibition is not deterrence at every margin, and the margin that matters here is the one occupied by a person who has already committed a hijacking or an abduction. For that

---

75. *License Plate Readers (LPR) Cameras*, Flock Safety, https://www.flocksafety.com/products/license-plate-readers (last visited Aug. 21, 2026).

76. 605 Ill. Comp. Stat. 140/5.

77. *Not All License Plate Readers Are Equal: When Plate Data Fails, How Do Investigations Continue?*, Flock Safety (Feb. 6, 2026), https://www.flocksafety.com/blog/not-all-license-plate-readers-are-equal-when-plate-data-fails-how-do-investigat (last visited Aug. 21, 2026).

78. 625 Ill. Comp. Stat. 5/3-703.

79. *Id.* 5/4-104(a)(4).

80. *Id.* 5/3-704(b)(4).

person the registration offense is not a cost. It is a rounding error attached to conduct already undertaken.

C. Substitution Is Cheaper Than Avoidance

The comparison that settles the question is between the two ways of defeating a reader network.

The first is avoidance, which requires knowing where the cameras are, accepting the routes that remain, and continuing to accept them for the duration of the exposure. It fails whenever the map is incomplete and it fails whenever the necessary destination sits behind a camera.

The second is substitution, which requires a plate. It works on every road, including roads the network covers most densely, and it requires no knowledge of the network at all. A British investigation found plates fabricated on request in ten minutes without the checks the law requires.[81]

Substitution therefore dominates avoidance for any offender motivated enough to do either, which means the population most determined to defeat the network defeats it at a point the network cannot observe. What remains inside the network is the population with no reason to leave it. That is not a criticism of the technology's accuracy. It is an observation about which people a system captures when the people it is aimed at can step out of it for the price of a plate.

D. Substitution Produces Misdirection, Not Invisibility

The final step is the one that returns this Part to the article's thesis, and it is the reason plate substitution is not merely a policy objection.

A substituted plate does not remove a vehicle from the record. The camera still reads. The database still writes. What changes is whose name the read resolves to. The offender does not become invisible; the offender becomes somebody else, and that somebody is a registered owner who was not present, has no notice, and holds no information with which to contest the entry.

---

81. *Number Plate Cloning: Fake Plates 'Ready in 10 Minutes'*, BBC News, https://feeds.bbci.co.uk/news/uk-england-birmingham-453 (last visited Aug. 21, 2026) (finding registered suppliers producing plates without verifying the buyer's right to the registration number).

The consequence is documented in the jurisdiction that adopted camera enforcement earliest. Reporting on an unpublished government study found that "thousands of innocent motorists are being wrongly accused of driving offences and more serious crimes because of the ease with which their vehicle's registration plate can be cloned by criminals or dishonest drivers seeking to avoid detection."[82] A companion account described the mechanism precisely: the notice "is sent to the unsuspecting owner of the vehicle, who then has to try to prove it was not their car involved in the offence."[83]

That is silent attribution operating as a tool rather than as an accident. The evasion is accomplished by causing the system to make a false attribution to a third party, and the system has no capacity to notice, because it has no field in which the attribution was ever recorded as an inference.

Illinois anticipated exactly this circumstance in the system that adjudicates a fine and supplied a remedy for it. A hearing officer may consider that the plates were stolen before the violation and not in the owner's possession, on proof that a report was filed with law enforcement.[84] The defense exists because the legislature understood that a plate read can land on a person whose plate was taken. No corresponding provision governs the reader network, where the same misdirected read is retained, shared, and queried with no notice to the person it names and no forum in which that person could invoke anything.

Nor is the error confined to deliberate substitution. Police in Minnesota stopped a driver in June 2026 after readers flagged his plate twice as stolen, which occurred because a California theft report had been entered into the national database with incomplete numbers.[85] An audit of the Los Angeles Police Department's use of the same vendor found officers had stopped

82. *Motorists Fall Prey to Cloned Registrations*, Daily Telegraph (Feb. 27, 2023), https://www.pressreader.com/uk/the-daily-telegraph/2 (last visited Aug. 21, 2026) (describing a report prepared by Home Office officials, the National Police Chiefs' Council, and the licensing agency).

83. *More Criminals Cloning Number Plates to Swerve Cameras Issuing Eco-Fines*, Daily Telegraph (Jan. 28, 2023), https://www.pressreader.com/uk/the-daily-telegraph/20230128/281758453424554 (last visited Aug. 21, 2026).

84. 625 Ill. Comp. Stat. 5/11-208.6(h)(1), (i).

85. *Flock Cameras Wrongly Flag Plates as Stolen, Lead to Police Stop in Plymouth*, CBS News Minnesota (July 12, 2026), https://www.cbsnews.com/minnesota/news/flock-cameras-wrongly-flag-plates-as-stolen (last visited Aug. 21, 2026).

161 vehicles incorrectly flagged as stolen within two months, and the department dropped the contract.[86] In each instance the record asserted something about a plate, the assertion was wrong, and the cost was collected from a body at the roadside rather than from the record.

E. Detection Runs Through the Victim

The remaining question is duration. A substituted plate defeats the network only for as long as it goes unnoticed, and an argument that ignores the detection interval proves nothing.

The interval is long, and the reason is that the two forms of substitution behave differently. A fabricated plate, corresponding to no valid registration, is what a reader network is genuinely good at catching, because the query returns nothing or returns a mismatch. A cloned plate, copied from a vehicle that is currently registered, taxed, insured, and on the road, returns a clean and accurate record every time it is read. There is nothing for the system to notice.

The practice migrated accordingly, and the migration is documented as a response to camera deployment. Reporting on the British experience describes offenders abandoning wholly false plates because automated checking defeats them, and turning instead to real registration numbers taken from vehicles with current documentation.[87] That is a surveillance architecture generating an evolutionary pressure and selecting the wrong outcome. Before the cameras, the evasion injured nobody in particular. After them, the evasion requires a victim.

Cloners choose the donor vehicle to match. Accounts of the practice describe offenders copying plates onto vehicles of the same model and color as the original,[88] which defeats by construction the countermeasure the vendor offers for plate unreliability. A check of make, color,

---

86. *See* Emma Camp, *She Spent 7 Months in Legal Hell After Cops Used Flock Surveillance To Identify the Wrong Car*, Reason (Aug. 2026), https://www.yahoo.com/news/us/articles/flock-cameras-license-plate-readers-140035485.html (last visited Aug. 21, 2026).

87. *See 10 Steps to Take If Your Number Plates Have Been Cloned*, Klick Plates, https://klickplates.com/news/22/10-steps-to-take-if-yo (last visited Aug. 21, 2026) (reporting the shift away from fabricated plates because automated plate checking defeats them, toward real numbers taken from vehicles current on registration, inspection, and insurance).

88. Glyn Moody, *Vehicle Cloning: Another Reason Not to Use Automated License Plate Readers*, Techdirt (Mar. 11, 2024), https://www.techdirt.com/2024/03/11/vehicle-cloning-another-reason-not-to-use-automated-license-plate-readers/ (last visited Aug. 21, 2026) (reporting British drivers discovering that the assumption of plate authenticity no longer holds, and that fines reach the plate's registered owner rather than the offender).

and body type against the registration record returns a match, because the offender selected the donor so that it would.

Detection therefore does not occur inside the system at all. It occurs when the falsely named owner opens the mail. Every account of the practice describes the same sequence: the victim learns of the cloning on receiving a citation for an offense committed somewhere the victim has never been.[89] The interval is bounded by the victim's correspondence, not by the network's capability.

The scale is measurable and it tracks camera density. Penalty notices cancelled on grounds of cloning by London councils rose from 22,450 in 2021 to 36,794 in 2023, and one borough attributed close to two percent of all its notices to cloned vehicles.[90] The transport authority recorded an increase of several hundred percent in notices overturned for cloning following the expansion of a camera-enforced charging zone.[91]

The British record is the right comparator, and not because British law governs. It is the jurisdiction that deployed dense camera enforcement earliest, at a reported eleven thousand readers producing on the order of one hundred million images daily,[92] which makes it the closest available observation of an American network at maturity.

One methodological point governs every figure above and cuts in a single direction. Each counted case is a case in which an innocent person successfully proved a negative about their own whereabouts and obtained a cancellation. Cases in which the falsely named owner could not

---

89. *See Thousands Hit by Fines from Cloned Car Plates*, BBC News, https://feeds.bbci.co.uk/news/articles/cd19pnky4x5o (last visited Aug. 21, 2026) (describing a driver who began receiving parking penalties in December 2022 for locations in central London while his vehicle was parked at his home nearly forty miles away).

90. *What to Do If Your Number Plate Is Cloned as Cases Jump 41 Percent*, Motoring Chronicle (June 18, 2026), https://motoringchronicle.com/what-to-do-if-your-number-plate-is-cloned-cases-jump-41-percent/ (last visited Aug. 21, 2026) (reporting figures obtained from London councils by BBC freedom of information request).

91. *Increase in Cloned Cars Leaving Innocent Drivers Facing Fines*, Fleet News (July 4, 2022), https://www.fleetnews.co.uk/news/fleet-industry-news/2022/07/04/increase-in-cloned-cars-leaving-innocent-drivers-facing-fines (last visited Aug. 21, 2026) (reporting a 631 percent rise in notices overturned for cloning following the zone expansion, and a consumer editor's assessment that the figures understate the problem because many drivers cannot produce the evidence to appeal).

92. *Motorists Fall Prey to Cloned Registrations*, *supra* note 82.

assemble that proof, or did not contest, or never learned what the record said about them, are not counted anywhere. The published numbers are a floor of unknown depth.

Which produces the finding this Part has been building toward. Against its least sophisticated subjects the network performs as advertised, because a person driving a vehicle registered in their own name is exactly what a plate read identifies. Against the offenders the network is sold on, it performs inversely, because the seriousness of the offense is what supplies the motive to adapt. And the system's integrity against its most motivated adversary rests, in the end, on the vigilance of the person it is falsely accusing.

VI. Consequences

A. Evidentiary Foundation

The most immediate consequence is evidentiary. A plate reader record is competent evidence that a vehicle bearing a given plate passed a given point at a given time. It is not evidence that a particular person was present, and the step from the first proposition to the second requires a separate foundation that is rarely laid and almost never contested.

The problem is not hearsay and it is not authentication. It is relevance and the chain of inferences: the proponent offers a record about an object to prove a fact about a person, and the connecting proposition is supplied by testimony, by argument, or by nothing at all. *Idris* supplies the answer to whether that connecting proposition can be established from the camera record itself. It cannot.[93]

The correct rule is modest and follows from existing law. Where plate reader evidence is offered to establish a person's location, the proponent should be required to identify the basis for the attribution, and the record should disclose whether the driver was observed. Where the attribution rests on registration alone, the evidence establishes the presence of the vehicle and

93. *Idris*, 552 F.3d at 566.

nothing further. *Glover* is not to the contrary; it holds that the inference is good enough to justify a brief investigative stop, not that it is good enough to place a person somewhere.[94]

B. Fourth Amendment

For search doctrine, the attribution gap cuts in a direction that may be uncomfortable for both sides.

It weakens one version of the privacy argument. If plate reads are records about vehicles, then the aggregation inquiry as *McCarthy* framed it is answering a question that the data does not pose, because the mosaic assembled is a mosaic of a household object.[95] A defender of the current architecture can say, accurately, that the government has not tracked anyone.

It strengthens a second version considerably. A system that produces assertions about people from observations of objects, at scale, retrospectively, with no observation of the person and no record that the observation was absent, is not a less intrusive form of surveillance. It is surveillance with an added and undisclosed error term, borne by people who are not suspected of anything and are frequently not present. *Chatrie* held that even brief digital location records fall within the Fourth Amendment because of what they reveal.[96] A record that reveals the wrong person's travel is not thereby less constitutionally significant.

The aggregation cases have measured density in cameras and duration in days.[97] The measure this article suggests is different and orthogonal: the proportion of a given person's recorded travel that the person actually performed. For most registered owners that proportion is high. For some it is zero.

---

94. *Glover*, 589 U.S. at 380–81.

95. *McCarthy*, 484 Mass. at 508–09, 142 N.E.3d 1090.

96. *Chatrie*, 609 U.S. ___, slip op. at 19–20.

97. *Compare McCarthy*, 484 Mass. at 508–09 (four cameras, two locations, one-year retention policy), *with Sturdivant*, 786 F. Supp. 3d at 1118 (twenty-six data points over six weeks).

C. Procedural Due Process

Automated traffic enforcement gives a person notice that an attribution has been made, tells that person what the attribution is, and provides a forum in which to answer.[98] It is not lavish process, and courts have called it sufficient.[99] But it satisfies the elementary requirement that notice be "reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections."[100]

The plate reader record supplies none of those. A registered owner receives no notice that a movement profile exists, no statement of what it asserts, and no forum in which to say that the assertions are about somebody else. Under *Mathews v. Eldridge*, the analysis turns on the private interest, the risk of erroneous deprivation under existing procedures together with the probable value of additional safeguards, and the government's interest.[101] The middle factor is the one that matters here, and it is unusual: the risk of error is not merely high in some cases but structurally unmeasurable in all of them, because the system records no information from which error could be detected.

The asymmetry sharpens when the same network's two populations are set side by side. Reads of a citizen's plate occur continuously, without complaint, suspicion, or notice. Misuse of those same reads by an officer becomes visible only when a person complains and an agency runs an audit of its query logs. A newspaper analysis of police and court records identified at least forty-six officers accused of using the network for unauthorized tracking, most of them surveilling women.[102] Those cases surfaced through the query log, which records who searched. Nothing in the architecture records anything to the person searched. The accountability surface faces the operator, and the subject of the record is not on it.

---

98. 625 Ill. Comp. Stat. 5/11-208.6(d)(10)(B), (h).

99. *Jacobsma*, 862 N.W.2d at 344–46; *Idris*, 552 F.3d at 567.

100. *Mullane v. Cent. Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950).

101. *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976).

102. *Flock Adds Safeguards to Licence-Plate Readers After Wave of Stalking Cases*, Al Jazeera (Aug. 14, 2026), https://www.aljazeera.com/news/2026/8/14/flock-adds-safeguards-to-licence-plate-readers-after-wave-of-stalking-cases (last visited Aug. 21, 2026) (reporting the findings of a Washington Post investigation).

The doctrinal obstacle is real and should be named. Whether a person has a protected liberty or property interest in the accuracy of a movement profile held by the government is unsettled, and a court could conclude that no cognizable interest attaches until the profile is used. That answer has a cost. It means the only person who can complain is the person against whom the record has already been deployed, which is to say the person whose complaint arrives after the harm.

D. The Population That Absorbs the Error

Every registered owner bears some share of the attribution error. One group bears all of it.

A person who holds title to a vehicle and does not drive it has a movement profile in these systems that is false in its entirety. The profile is not partly inaccurate. Every entry belongs to someone else. Title is commonly held that way for ordinary reasons: financing, insurance rating, inheritance, or a household arrangement in which the person who cannot drive is the person who owns the asset.

Disabled people are disproportionately represented in that group, because the reasons a person does not drive are frequently reasons of disability, including conditions that make operating a vehicle unsafe or impossible and conditions that make leaving the home difficult. The error is total for them, they have no way to learn that the record exists, and they have no mechanism to correct it if they did. They also cannot mitigate it. A person can decline to carry a phone. A person cannot decline to be the registered owner of the household vehicle without giving up the asset, and cannot alter the plate without committing an offense.

The consequence runs in the other direction as well. Because the flag attaches to the plate rather than to a driver, the physical risk of a false attribution transfers to whoever is actually behind the wheel. An alert generated against an owner is served on a body that was never in the record.

E. What the Reforms Reach

The reforms currently on offer do not reach any of this. In August 2026 the dominant vendor, responding to documented misuse by officers, reduced its recommended default retention period from thirty days to seven, introduced a mode permitting longer retention for exceptional cases, and permitted agencies to restrict which offenses would allow another agency to query their cameras.[103] Model legislation has proposed a warrant requirement for data older than twenty-four hours.[104] Every one of those measures governs how long a record is kept, who may retrieve it, and on what showing. Not one of them governs whether the record says what it appears to say.

That the reforms cluster on duration is not an accident. Duration is the variable the case law measures. *McCarthy* counted cameras and weighed a one-year retention policy;[105] *Sturdivant* counted twenty-six data points across six weeks.[106] A shorter window is therefore a defense aimed squarely at the aggregation theory, and it is aimed at nothing else. The attribution error is made at the query and is indifferent to how much history preceded it.

It is also indifferent to the clock in a second way. Retention governs the vendor's database. It does not govern the copy. A read pulled inside the window and written into a report, an affidavit, an alert, or another agency's file survives whatever the source does, and the statutes that cap retention say so in terms: Maine's twenty-one day limit reaches only data that is not "intelligence and investigative record information."[107] The record that names a person is the record that has already left.

A shorter window does raise a question the industry has not answered. Either seven days is sufficient for the investigative purpose the networks are sold on, in which case every additional day was surplus that vendors and agencies defended as necessary, or it is not sufficient, in which

103. *Flock Adds Safeguards to Licence-Plate Readers After Wave of Stalking Cases*, *supra* note 102.

104. *See* Camp, *supra* note 86 (describing the Institute for Justice's Plate Privacy Project and its proposed warrant threshold).

105. *McCarthy*, 484 Mass. at 508–09, 142 N.E.3d 1090.

106. *Sturdivant*, 786 F. Supp. 3d at 1118.

107. Me. Rev. Stat. tit. 29-A, § 2117-A(5).

case agencies will invoke the mode permitting longer retention and the reform is a default setting rather than a limit. Both answers cost something previously asserted.

The experiment has in fact already been run. Sixteen states cap retention by statute, at intervals ranging from three minutes to one year.[108] New Hampshire draws the line where this article would draw it. Plate records must be "purged from the system within 3 minutes of their capture in such a manner that they are destroyed and are not recoverable," unless the read produced an arrest, a citation, or protective custody, or matched a vehicle named in a missing person or wanted broadcast.[109] That exception preserves the real-time alerting function in full and discards the retrospective archive entirely, which is a legislative judgment that retention buys only the second thing.

What the industry thinks those days are worth is on the record. When a Virginia bill's sponsor reduced a proposed cap from thirty days to twenty-one, police and sheriffs' associations withdrew their support and testified against the measure.[110] Eight days.

The empirical record is not thin, and it does not answer the question. A decade of public records work has produced hit ratios, network audits, and search logs at scale. On average roughly one half of one percent of plate scans matched a hot list at the moment of capture, which is to say that 99.5 percent of the plates collected were unconnected to any public safety interest when they were read.[111] Datasets covering more than twelve million logged searches by more than 3,900 agencies over eleven months are in public hands.[112] And the leading investigative evaluation found improvements in auto theft and robbery clearances after nearly one hundred

---

108. Va. State Crime Comm'n, *Law Enforcement Use of Automatic License Plate Recognition* (2024) (listing statutory retention periods including New Hampshire at three minutes, Utah at fourteen days, Maine at twenty-one days, Georgia at thirty days, California and Minnesota at sixty days, and Vermont at one year).

109. N.H. Rev. Stat. Ann. § 261:75-b(VIII).

110. *License Plate Reader Bill Survives, but Surveillance Concerns Loom*, https://www.yahoo.com/news/license-plate-reader-bill-survi (last visited Aug. 21, 2026).

111. Elec. Frontier Found., *Data Driven: What We Learned*, https://www.eff.org/pages/what-we-learned (last visited Aug. 21, 2026).

112. Elec. Frontier Found., *EFF's Investigations Expose Flock Safety's Surveillance Abuses: 2025 in Review* (Dec. 2025), https://www.eff.org/deeplinks/2025/12/effs-investigations-expose-flock-safetys-surveillance-abuses-2025-review (last visited Aug. 21, 2026) (reporting that California agencies searched a single city's database 3,965,519 times over roughly one year).

fixed readers were installed, none of which reached statistical significance in multivariate analysis.[113]

What none of that record contains is the age of the data returned by a query that produced a lead, and the reason is structural rather than accidental. The audit log preserves the search and not its result. It records the date, the officer, the plate searched, the reason typed, and the number of cameras reached; in one department twenty-eight percent of 15,335 logged searches recorded no reason at all.[114] It records nothing about whether the search found anything, and nothing about whether what it found was right. The accountability apparatus built around this technology has the same gap as the technology itself. It documents the act and never the accuracy.

VII. Conclusion

The question this article raises has an answer already, and the answer is on the books.

Illinois has written into statute that a registered owner may not have been in possession of the vehicle, and has provided defenses on that basis in two circumstances.[115] The Seventh Circuit has found that roadside camera technology is unlikely to establish who was driving and that a municipality would be essentially unable to prove it.[116] The Supreme Court of Missouri has struck down a camera ordinance for shifting onto the owner the burden of proving that he was not the operator.[117] And the Supreme Court of the United States has held that an officer may act on the owner-driver inference for the limited purpose of a brief stop, in circumstances where looking at the driver will dispel it.[118] Taken together, that is a considered legal judgment that a plate identifies a vehicle, that the operator is a separate question, and that the inference between them is worth about as much as a momentary suspicion.

---

113. Christopher S. Koper & Cynthia Lum, *The Impacts of Large-Scale License Plate Reader Deployment on Criminal Investigations*, 22 Police Q. 305 (2019).

114. *What the Audit Log Reveals*, DeFlock Apex, https://deflockapex.org/audit (last visited Aug. 21, 2026) (compiling audit records published under state transparency laws).

115. 625 Ill. Comp. Stat. 5/11-208.6(h)(1), (h)(1.5).

116. *Idris*, 552 F.3d at 566.

117. *Tupper*, 468 S.W.3d at 364.

118. *Glover*, 589 U.S. at 380, 385.

Plate reader doctrine has proceeded without that judgment. It asks whether a plate is exposed to public view, and answers correctly that it is.[119] It asks whether accumulated points reconstruct the whole of a person's movements, and answers by counting cameras.[120] It does not ask whose movements are being reconstructed, and the two leading decisions do not reach the question.[121]

A record that asserts a person was somewhere, generated by a device that never saw a person, carrying no field in which the absence of that observation could be noted, is not a record of a person's movements. It is a record of a vehicle's movements with a name written on it by someone who was not there.

119. *Class*, 475 U.S. at 114.

120. *McCarthy*, 484 Mass. at 508–09, 142 N.E.3d 1090.

121. *Id.*; *Scholl*, 776 F. Supp. 3d at 712–14, 719.

References

Al Jazeera. (2026, August 14). *Flock adds safeguards to licence-plate readers after wave of stalking cases*.

Automated Traffic Law Enforcement Systems, 625 Ill. Comp. Stat. 5/11-208.6.

Bennis v. Michigan, 516 U.S. 442 (1996).

British Broadcasting Corporation. (n.d.). *Number plate cloning: Fake plates 'ready in 10 minutes'*.

British Broadcasting Corporation. (n.d.). *Thousands hit by fines from cloned car plates*.

Camp, E. (2026). *She spent 7 months in legal hell after cops used Flock surveillance to identify the wrong car*. Reason.

Cardwell v. Lewis, 417 U.S. 583 (1974).

Carpenter v. United States, 585 U.S. 296 (2018).

CBS News Minnesota. (2026, July 12). *Flock cameras wrongly flag plates as stolen, lead to police stop in Plymouth*.

Certificates of Title and Registration of Vehicles, 625 Ill. Comp. Stat. 5/3-703, 5/3-704, 5/4-104.

Chatrie v. United States, 609 U.S. ___ (2026).

City of Creve Coeur v. Nottebrok, 356 S.W.3d 252 (Mo. Ct. App. 2011).

City of Knoxville v. Brown, 284 S.W.3d 330 (Tenn. Ct. App. 2008).

City of Sioux City v. Jacobsma, 862 N.W.2d 335 (Iowa 2015).

City of St. Peters v. Roeder, 466 S.W.3d 538 (Mo. 2015).

Commonwealth v. Govan, 259 N.E.3d 370 (Mass. 2025).

Commonwealth v. Long, 152 N.E.3d 725 (Mass. 2020).

Commonwealth v. McCarthy, 484 Mass. 493, 142 N.E.3d 1090 (2020).

Daily Telegraph. (2023, February 27). *Motorists fall prey to cloned registrations*.

Daily Telegraph. (2023, January 28). *More criminals cloning number plates to swerve cameras issuing eco-fines*.

DeFlock Apex. (n.d.). *What the audit log reveals*.

Department of Housing & Urban Development v. Rucker, 535 U.S. 125 (2002).

Electronic Frontier Foundation. (2025, December). *EFF's investigations expose Flock Safety's surveillance abuses: 2025 in review*.

Electronic Frontier Foundation. (n.d.). *Data driven: What we learned*.

Expressway Camera Act, 605 Ill. Comp. Stat. 140/5.

Ferguson, A. G. (2017). The smart Fourth Amendment. *Cornell L. Rev.*, 102, 547.

Fleet News. (2022, July 4). *Increase in cloned cars leaving innocent drivers facing fines*.

Flock Safety. (2026, February 6). *Not all license plate readers are equal: When plate data fails, how do investigations continue?*

Flock Safety. (n.d.). *License plate readers (LPR) cameras*.

Gaines, J. (2026, January 9). *Finding 67 Flock Safety live PTZ camera and LPR feeds and debug web interfaces accidentally exposed without authentication to the internet*.

Gatewood, J. C. (2013). It's raining Katz and Jones: The implications of United States v. Jones, a case of sound and fury. *Pace L. Rev.*, 33, 683.

Heller v. Brookhaven Borough, No. 2:25-cv-05550 (E.D. Pa. Feb. 11, 2026).

Idris v. City of Chicago, 552 F.3d 564 (7th Cir. 2009).

Illinois v. Wardlow, 528 U.S. 119 (2000).

Kansas v. Glover, 589 U.S. 376 (2020).

Kerr, O. S. (2012). The mosaic theory of the Fourth Amendment. *Mich. L. Rev.*, 111, 311.

Klick Plates. (n.d.). *10 steps to take if your number plates have been cloned*.

Koebler, J. (2025, December 22). Flock exposed its AI-powered cameras to the internet. We tracked ourselves. *404 Media*.

Koper, C. S., & Lum, C. (2019). The impacts of large-scale license plate reader deployment on criminal investigations. *Police Q.*, 22, 305.

Krieger v. City of Rochester, 42 Misc. 3d 753 (N.Y. Sup. Ct. 2013).

Mathews v. Eldridge, 424 U.S. 319 (1976).

Moody, G. (2024, March 11). Vehicle cloning: Another reason not to use automated license plate readers. *Techdirt*.

Motor Vehicles, Me. Rev. Stat. tit. 29-A, § 2117-A.

Motoring Chronicle. (2026, June 18). *What to do if your number plate is cloned as cases jump 41 percent*.

Mullane v. Central Hanover Bank & Trust Co., 339 U.S. 306 (1950).

New York v. Class, 475 U.S. 106 (1986).

9News. (2025, December 23). *Douglas County's Flock camera compromised as company leaves it exposed on internet*.

Number Plate Scanning Devices, N.H. Rev. Stat. Ann. § 261:75-b.

Riley v. California, 573 U.S. 373 (2014).

Sandstrom v. Montana, 442 U.S. 510 (1979).

Scholl v. Illinois State Police, 776 F. Supp. 3d 701 (N.D. Ill. 2025).

Spencer, S. B. (2018). *Predictive surveillance and the threat to Fourth Amendment jurisprudence*. SSRN. https://doi.org/10.2139/ssrn.3195977

Straight Arrow News. (2025, December 22). *Flock camera captured kids on a playground. A security failure exposed them online*.

Tupper v. City of St. Louis, 468 S.W.3d 360 (Mo. 2015).

United States v. Boyle, 469 U.S. 241 (1985).

United States v. Cortez, 449 U.S. 411 (1981).

United States v. Jones, 565 U.S. 400 (2012).

United States v. Knotts, 460 U.S. 276 (1983).

United States v. Sturdivant, 786 F. Supp. 3d 1098 (N.D. Ohio 2025).

United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021).

Van Harken v. City of Chicago, 103 F.3d 1346 (7th Cir. 1997).

Virginia State Crime Commission. (2024). *Law enforcement use of automatic license plate recognition*.

Washington v. Glucksberg, 521 U.S. 702 (1997).

Wostbrock, M. (2024). Miller in a cashless society: Financial surveillance and the Fourth Amendment. *Colum. Bus. L. Rev.*, 2023(2). https://doi.org/10.52214/cblr.v2023i2.12487

Wyden, R. (2025, November 3). *Letter to Chairman Andrew N. Ferguson, Federal Trade Commission*. United States Senate.