

The Plate Is Not the Person

What Owner Liability Already Concedes About Automated Vehicle Surveillance

A camera records a plate. A database turns that into a claim about where a person has been. Nothing in between ever checks whether that person was in the car.

THE MOVE NOBODY NAMES

Somewhere between the camera and the file, an object becomes a person

A camera at the roadside reads a registration plate. A database turns that reading into a statement about where somebody has been. At no point does anything in that chain establish that the somebody was ever in the vehicle.

This paper gives that conversion a name, calls the space it jumps across the attribution gap, and argues that American law has already worked through both of them, in a place nobody has thought to look.

WHERE THE ANSWER ALREADY IS

Traffic camera law admits the whole thing, three times over

The place to look is automated traffic enforcement, which has been arguing about exactly this since long before anybody built a reader network. Its statutes and its case law concede, in writing, that a camera cannot tell you who was driving.

Plate reader doctrine has grown up as though none of that had ever happened.

The Admission

read the statutes as evidence rather than as rules



Nobody drafts that clause about a system that produces the driver's name.

FIRST ADMISSION

Liability without regard to who was driving

Illinois provides that unless an officer handed a citation to the driver at the scene, the vehicle's owner is the one who pays. Local ordinances say it more bluntly still. An appeals court in Missouri looked at one that made responsibility a matter of who owns the car, and said in terms that it made no difference whether that person had been driving. A Tennessee court put it the same way, rejecting the argument that the city had to establish who was in control.

Read those as evidence rather than as rules. A statute assigning liability without regard to who was driving is a legislature recording that it cannot find out who was driving.

**Nobody drafts that clause about a system which produces the driver's name.
The provision exists because the camera's record stops at the vehicle.**

SECOND ADMISSION

And the defences say it twice more, precisely

There is a way out in Illinois if the car or its plates had been stolen before the offence and were neither controlled nor held by the owner when it happened, and a second one if the car was hijacked. Both require producing evidence that the theft was reported to a force.

That phrase is the owner-driver divergence set down in statutory language. The legislature knew the owner may well not have been in the car, wrote it down, and then made the divergence count in exactly two situations, both needing a crime by a third party and a police report.

Have your car taken by a stranger and the law will listen when you say you were not driving. Have it taken by your husband and the law declines to enquire. The same thing is true in both households. Only one of them gets a hearing.

THIRD ADMISSION

A federal appeals court made it a finding of fact

Owners argued that Chicago's ordinance unconstitutionally charged them even where they had not been driving. The Seventh Circuit affirmed dismissal, and the operative passage is about what the technology can do rather than about municipal power. Fining the owner is rational, the court reasoned, since the equipment is good at establishing which vehicles went through the light and much worse at establishing who was at the wheel, which would leave owners free to blame a friend or a child and leave the city with no realistic way of contradicting them.

That is not a throwaway line. The ordinance's rationality rests on it, and without it the constitutional analysis falls over.

WHAT THE REGIME PAYS FOR IT

Every comparison the court reached for is candid about what it is doing

The court placed camera enforcement in a line of no-fault penalty regimes: forfeiting a vehicle used in a crime, evicting a tenant over a guest's conduct, taxing somebody for an adviser's mistake. Each of those names a party who did not do the thing and explains why they should pay anyway.

Being open about it is exactly the point. Declare that you are running a scheme without fault and you invite people to say so. The court leaned as well on how little was at stake, putting the interest involved at ninety dollars over a traffic offence.

The Same Inference, Unbounded

what plate reader doctrine asks, and what it never asks



Both leading questions assume the vehicle's movements are the person's, and neither defends it.

THE TWO QUESTIONS COURTS ASK

Neither one reaches the premise

Is a plate exposed to public view?

The plain view line asks whether somebody driving on a road has any expectation of privacy in a number bolted to the outside of their car. Usually the answer is no.

Do enough points reconstruct a life?

The aggregation line asks whether accumulated location readings assemble a picture of the whole of somebody's movements, which is the theory the case law has actually been developing.

Each question assumes, without saying so, that a car's journeys are its owner's journeys. The main decisions never argue for that assumption, and the reason is straightforward. They never arrive at it.

THE CASE THAT AUTHORISED THE INFERENCE

Three conditions, and a database removes all of them

The Supreme Court permitted an officer to infer that a registered owner is the person driving. It did that solely for the purpose of reasonable suspicion, solely where nothing known cuts the other way, and solely in circumstances where an officer with eyes on the driver can rule it out on the spot.

Retrieval from a database strips out every one of those. It is not a brief roadside inference by somebody who can see through the windscreen. It is a query returning a name, with nobody looking at anyone.

That decision holds the inference good enough to justify stopping a car for a moment. It does not hold it good enough to place a person somewhere.

Where The Conversion Happens

and why no part of the system records it



No stage of retrieval marks the moment an observation of a vehicle becomes a claim about a person.

LOCATING IT

Nothing writes down the moment the object becomes somebody

A vehicle is what the camera captures. A vehicle is what gets stored. A vehicle is what comes back when somebody searches. Then a human being's name turns up in a report, a sworn statement, an alert, or another force's paperwork, and nowhere in the system does any field mark that something happened in between.

That is what makes the attribution silent. It is not concealed. It is simply never written down, so nobody has to defend it and nobody can contest it.

The Justification

test it on its own terms, because it is why the contracts get renewed



Swapping a plate beats a reader network more cheaply than avoiding one.

THE VENDOR'S OWN WORDS

The company has already conceded the premise in writing

The commercial case rests on an unstated assumption: that the plate identifies the vehicle. The party with most to lose from doubting that has put the doubt in print itself.

Writing for a technical audience in February 2026, the biggest supplier granted that you cannot always trust a plate, listing the ways: switched between cars, obscured, forged, taken, tampered with, read wrongly by the machine, swapped for a temporary or paper tag, or on occasion simply illegible.

The post exists to sell a supplementary identification product, and its frankness serves that purpose. It remains an admission, by the operator of the largest such network, that the identifier everything rests on is defeated routinely and by ordinary means.

TWO WAYS TO BEAT A CAMERA NETWORK

One of them dominates the other

Avoidance

This means learning every camera position, taking whichever roads remain, and going on taking them for however long the exposure lasts. Miss one camera and it collapses. Need to reach somewhere a camera covers and it collapses again.

Substitution

You need a plate. It works on every road, including the ones the network covers most heavily, and it requires knowing nothing at all about where the cameras are.

Reporters in Britain found firms turning out plates to order inside ten minutes, skipping the verification the law demands. Putting a plate on a car it was not issued for is unlawful in Illinois, and the registration can be revoked for it. To somebody who has already carried out a hijacking or taken a person, that offence deters nothing. It is loose change beside what they have already chosen to do.

AND HERE IS THE STING

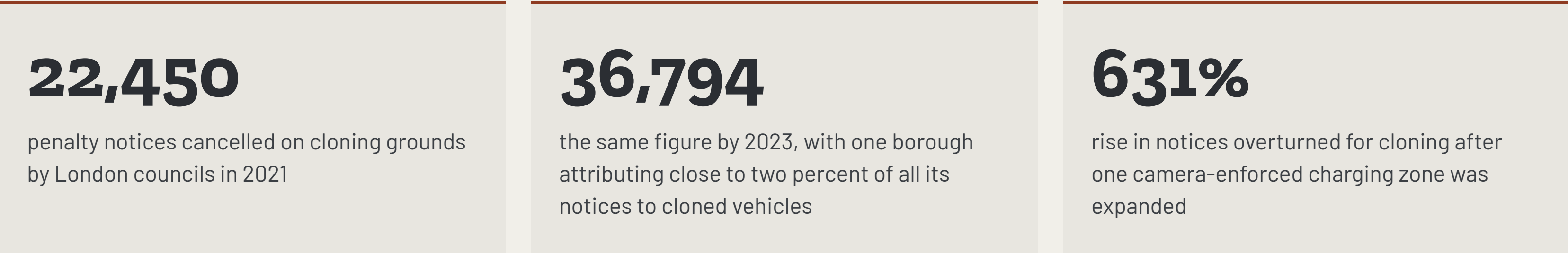
A swapped plate does not make you invisible. It makes you somebody else.

Nothing stops the camera reading. Nothing stops the database recording. The single thing that alters is which person the reading ends up pointing at.

Whoever did it has not disappeared from the file. They have turned into some registered owner who was elsewhere, has been told nothing, and possesses no material with which to argue. The system cannot detect it, and the person falsely named finds out by post.

MEASURED WHERE IT STARTED EARLIEST

The scale tracks camera density



The reason to look at Britain is not that its law applies here. It is that Britain built dense camera enforcement before anyone else, running a reported eleven thousand readers and generating on the order of a hundred million images every day. That makes it the closest available look at an American network once it matures.

SOURCES *What to Do If Your Number Plate Is Cloned as Cases Jump 41 Percent*, Motoring Chronicle (June 18, 2026); *Increase in Cloned Cars Leaving Innocent Drivers Facing Fines*, Fleet News (July 4, 2022).

ONE METHODOLOGICAL POINT

Every number here counts only the people who won

Each case in those figures is one where an innocent person managed to prove a negative about their own whereabouts and got the notice cancelled.

Whoever failed to put that evidence together, or let it go, or never discovered what was written about them, is counted nowhere at all.

The published figures are a floor of unknown depth.

THE FINDING THIS PART WAS BUILDING TO

The network works inversely to how it is sold

Against its least sophisticated subjects it performs exactly as advertised, because somebody driving a car registered in their own name is precisely what a plate reading identifies.

Against the offenders it is sold on, it performs the other way round, because the seriousness of the offence is what supplies the motive to adapt.

Which leaves the network's soundness against the people most determined to beat it resting on how alert the wrongly accused happen to be.

Consequences

evidence, and the people who absorb the error



One group's recorded travel is false in every single entry.

IN COURT

The record proves a vehicle was there, and stops

What the record proves is that some vehicle wearing a particular number went past a particular spot at a particular moment. It proves nothing about who was inside. Bridging those two takes a separate showing that hardly ever gets made and almost never gets contested.

Neither hearsay nor authentication is what is wrong here. What is wrong is relevance, and the run of inferences behind it. A document about a thing is being put forward to establish a fact about a human being, and whatever links the two arrives by way of a witness, by way of submissions, or by way of nothing whatever.

The rule that follows is modest. When this material is put forward to establish that somebody was in a particular place, require whoever offers it to say what the identification rests on, and require the file to show whether any human being laid eyes on the driver.

THE PEOPLE WHO ABSORB IT

Every owner carries some of the error. One group carries all of it.

Hold the registration on a car you never drive and the travel history these systems keep on you is wrong from top to bottom. Not partly. Line by line, all of it describes somebody else's journeys. Registrations sit like that for entirely mundane reasons. A loan requires it. The insurance is cheaper. Somebody died. Or the household is arranged so that the person unable to drive is the one whose name is on the car.

That group contains disproportionately many disabled people, since not driving usually has a disability behind it, whether a condition making it dangerous or impossible to control a car or one that makes going out at all difficult.

The error is total for them, they have no way of learning the record exists, and no mechanism to correct it if they did.

AND THEY CANNOT OPT OUT

You can decline to carry a phone. You cannot decline to own the car.

There is nothing such a person can do to reduce it. Handing back the registration means handing over the car, and changing the plate is against the law.

The consequence also runs the other way. The alert is hung on a number, not on a driver, so the bodily danger created by a wrong name lands on whoever happens to be at the wheel. An alert raised in one person's name gets executed against somebody who never appeared in the file at all.

WHY THE REFORMS MISS

Everything on offer governs the clock, not the meaning

August 2026 brought changes from the main supplier, prompted by recorded abuse of the system by officers: the suggested default storage period dropped from a month to a week, an option appeared for keeping things longer in unusual cases, and forces gained the ability to specify which offences would let another force search their cameras. Model legislation has proposed a warrant requirement for anything older than twenty-four hours.

All of it concerns storage periods, who is allowed to search, and what they must show first. None of it concerns whether what is stored means what everyone assumes it means.

The clustering on duration is not an accident. Duration is the variable the case law measures, so a shorter window is a defence aimed squarely at the aggregation theory, and at nothing else.

AND RETENTION DOES NOT REACH THE COPY

The record that names a person has already left the database

Retention rules govern the vendor's own store. They do not govern the copy. Take a reading out before the deadline, put it in a report, a sworn statement, an alert, or a file at another force, and it survives whatever becomes of the original. The retention statutes admit as much on their face: one state's three-week cap applies only to material that has not become intelligence or investigative record information.

So the entry that turned a vehicle into a person is precisely the entry the clock never touches.

THE CLAIM, RESTATED

Three things this paper found

One: an admission, in statute and in decided cases, that a number plate does not tell you who was driving, sitting inside the very jurisdictions that treat plate data as a record of where somebody went. Second, that no stage of retrieval records the moment an observation of a vehicle becomes a claim about a person. Third, the group whose recorded travel is false in its entirety: registered owners who do not drive.

None of it requires a new theory of privacy. It requires reading two bodies of law that have been sitting a few feet apart for twenty years.

The camera reads a plate. The plate is not the person. Everything downstream has been proceeding as though it were.

REFERENCES

References

Travis Gilly, *The Plate Is Not the Person: What Owner Liability Already Concedes About Automated Vehicle Surveillance*, August 2026.

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.