DEEP DIVE

Bootleggers, Cops, and Cars: How Driving Became a Privacy Trap

April 14, 2025, 5:00 AM

By Cassandre Coyer, Tonya Riley and Jorja Siemons

Chief Petty Officer Lee Schmidt was stuck in morning traffic en route from Norfolk, Va., to his job in Virginia Beach when he first noticed the "weird little camera" outside a CVS: an automated license plate reader.

Schmidt began seeing the cameras everywhere after that first sighting in late 2023—outside banks, near schools, and "just to get on the interstate" heading to work. "You cannot dodge these," said Schmidt, now retired from his Navy electronics technician job. "It's nearly impossible."

Norfolk Police Chief Mark Talbot painted a similar picture when briefing officials shortly after Norfolk installed 172 license plate reading cameras across the city earlier that year. "It would be difficult to drive anywhere of any distance without running into a camera somewhere," he said, according to an account in The Virginian-Pilot.

But that's where their accounts diverge.

Schmidt is suing Norfolk claiming the cameras used in tandem create a dragnet of sorts violating the Fourth Amendment's prohibition against unreasonable searches and seizures.

Norfolk and its police maintain the license plate readers enhance public safety and are legal, and deny they're used to follow its 230,000 residents.

The court battle is one front in an issue gaining national significance. About 1,800 police departments operate automated license plate readers, according to the Electronic Frontier Foundation, in addition to thousands of municipalities, homeowner associations and private businesses.

More than 14,000 license plate cameras are now operating across the country, according to the open source, anti-surveillance project DeFlock. And because of legal precedent dating back decades, police don't usually need a warrant to get the information those devices are collecting.

Privacy inside automobiles is also becoming more tenuous as technology expands. Drivers and passengers in late-model cars leave digital breadcrumbs with almost everything they do, information that is also easily obtained by police.

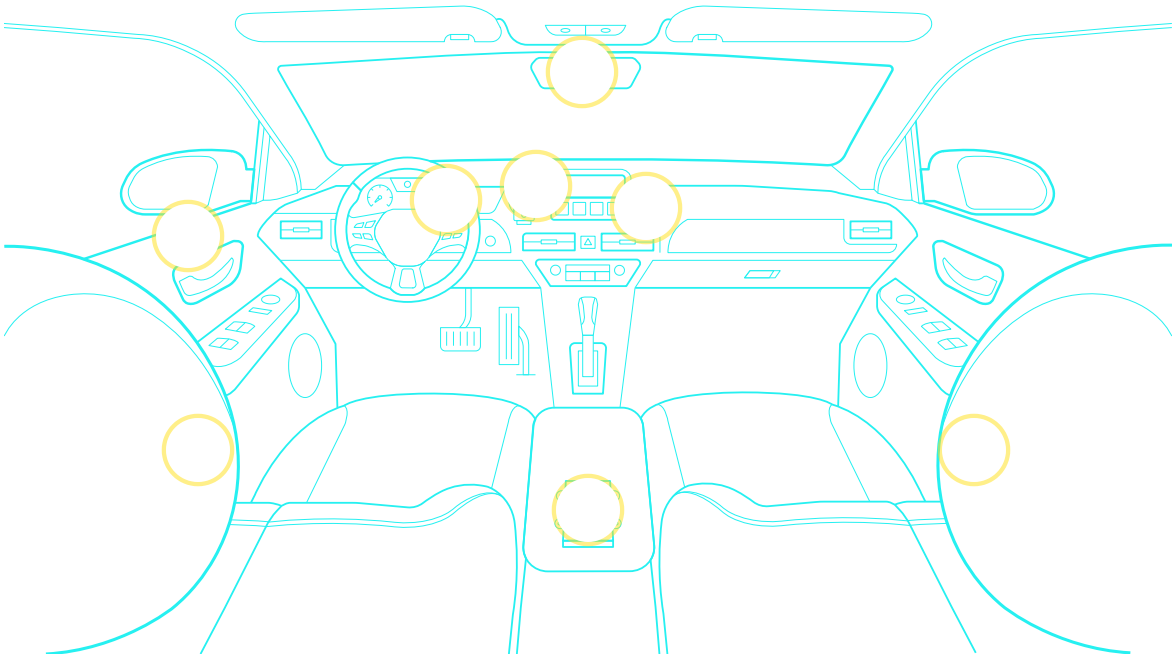
Once symbols of freedom and the open road, the cars we drive and the highways we travel have become privacy traps, according to legal advocates.

"You've just got these kind of surveillance bombs sitting in our world now that can collect so much information, and be accessed by local, state, federal, or foreign law enforcement," said Jen Caltrider, consumer advocate and former program director of Privacy Not Included at Mozilla Foundation, which led a report on car privacy.

"The concern is what is being done about it," Caltrider said. "From what I can tell, not enough."

Data a Modern Car Can Collect

A look at the various types of data collected by sensors within cars and external cameras pointed at them.



Source(s): Bloomberg Law Reporting

Bloomberg Law

Graphic: Jonathan Hurtarte, Jon Meltzer and Atthar Mirza/Bloomberg Law

License plate readers emerged in the US in the 1980s as a counter-terrorism measure, at first too bulky and costly for widespread use. Forty years later, the cameras are tiny, inexpensive, and discreetly mounted on light posts, buildings, and bridges.

Every police department in the country in a city with more than a million residents surveyed relies on license plate readers to gather evidence, identify suspects, facilitate crime scene analysis, or for traffic compliance, the Justice Department reported in 2020.

Devices from companies like Flock Safety and Motorola Solutions work by capturing an image of a vehicle and its license plate. The picture is then converted into a form of readable text using automated data extraction that can quickly be matched with vehicles of interest to police.

The cameras also capture a car's make and model, read its bumper stickers, and record the time and place the vehicle passed by. Motorola Solutions markets its cameras and database to police as able to "find the needle in a haystack" and predict "a best-address location and time-of-day, day-of-week heat map to determine when the vehicle is most likely to be there." Motorola didn't respond to requests for comments.

"It's been a bit of a game changer from a law enforcement perspective," Canyon County, Idaho Sheriff Kieran Donahue, president of the National Sheriffs' Association, told Bloomberg Law.

Donahue's office used the technology to find a girl who had been solicited on the dark web, he said. Police in Collin County, Texas, say they use it to monitor human traffickers, stolen vehicles, and cartels down the I-10 corridor. And Norfolk reported a 40% drop in stolen vehicles between 2023 and 2024, after it deployed the Flock cameras.

Police who have deals with automated license plate reader companies can access the databases where the information they collect is stored. And those databases can be shared among law enforcement agencies that opt in.

In the case of Flock, private customers like HOAs and neighborhoods can share camera access, too, but only with their local law enforcement agency.

License plate-scanning cameras and E-ZPass readers monitor traffic at Columbus Circle in New York City on Jan. 3, 2025. Photographer: Michael Nagle/Bloomberg via Getty Images

Illinois State Police and several state officials faced claims similar to Norfolk over "the retention and storing of the data, the long-term tracking of basically everyone who drives a car and just holding on to it, just in case one day they decide they don't like you," said Reilly Stephens, counsel at the Liberty Justice Center, who represents the plaintiffs in the Illinois case.

Some states are starting to limit how long the data is stored.

California largely prohibits highway patrol from keeping license plate reader data for more than 60 days. Colorado sets the bar at three years. Minnesota requires the establishment of written policies governing how the data is being used. A Virginia effort to require deletion of data after 21 days is awaiting final action from the governor after the legislature rejected his suggested changes. And lawmakers in several other states are debating the issue this year.

But most law enforcement agencies still can decide how long they retain the data and who can access it.

“They don’t have to go to a judge, they don’t get a warrant,” said Stephens. “They don’t have to show that they have a reasonable suspicion or any suspicion.”

Fourth Amendment

Drivers historically have enjoyed few privacy rights on the road.

In 1925, during the height of Prohibition, the Supreme Court established the automobile exception to the Fourth Amendment, saying police with probable cause could search cars without a warrant to catch bootleggers. A century later, the *Carroll v. United States* shield still applies.

Police can “take apart the upholstery, the spare tire, the gas tank,” said Adam Gershowitz, a professor at William & Mary Law School, where he specializes in criminal law. For modern vehicles “they can just plug a machine into this thing and extract a bunch of data from it.”

In the 1980s, after police hid a beeper in a car transporting chloroform across state lines, the Supreme Court held in *United States v. Knotts* that drivers have no reasonable expectation of privacy on public roads, even if police use technology to augment “their sensory faculties.”

More than four decades later, this remains at the core of the defense of license plate readers’ use in court.

“There’s no expectation of privacy in a vehicle or its license plate traveling on a public road,” said Andrea Korb, director of policy at license plate reader provider Flock Safety.

But plaintiffs in Illinois and Norfolk argue that *Knotts* shouldn’t hold up today. They cite the 2018 ruling *Carpenter v. United States,* when the Supreme Court reviewed law enforcement’s use of cellphone geolocation data under the Fourth Amendment and ruled that government needs a warrant to access a person’s cellphone location history, and cannot track this information indefinitely.

The case set precedent for other surveillance technologies that automated license plate surveillance should fall under, the plaintiffs argue.

They also point to a 2021 Fourth Circuit ruling citing *Carpenter* in another case, where judges found that the Baltimore Police Department’s use of planes equipped with surveillance cameras violated rights to privacy and free association under the First and Fourth Amendments. Because the aerial surveillance let police deduce “the whole of individuals’ movements,” the warrantless search was akin to attaching “an ankle monitor to every person in the city” and violated the Fourth Amendment, the court ruled.

That’s essentially what Norfolk police are doing with its fleet of license plate readers, argued Michael Soyfer, an attorney with the Institute for Justice and counsel for plaintiffs in the Norfolk case. Courts need to look at automatic license plate readers not just as individual cameras but as a surveillance apparatus that can track people’s movements and associations, he said.

Norfolk police say their cameras enhance public safety and don’t constitute continuous surveillance.

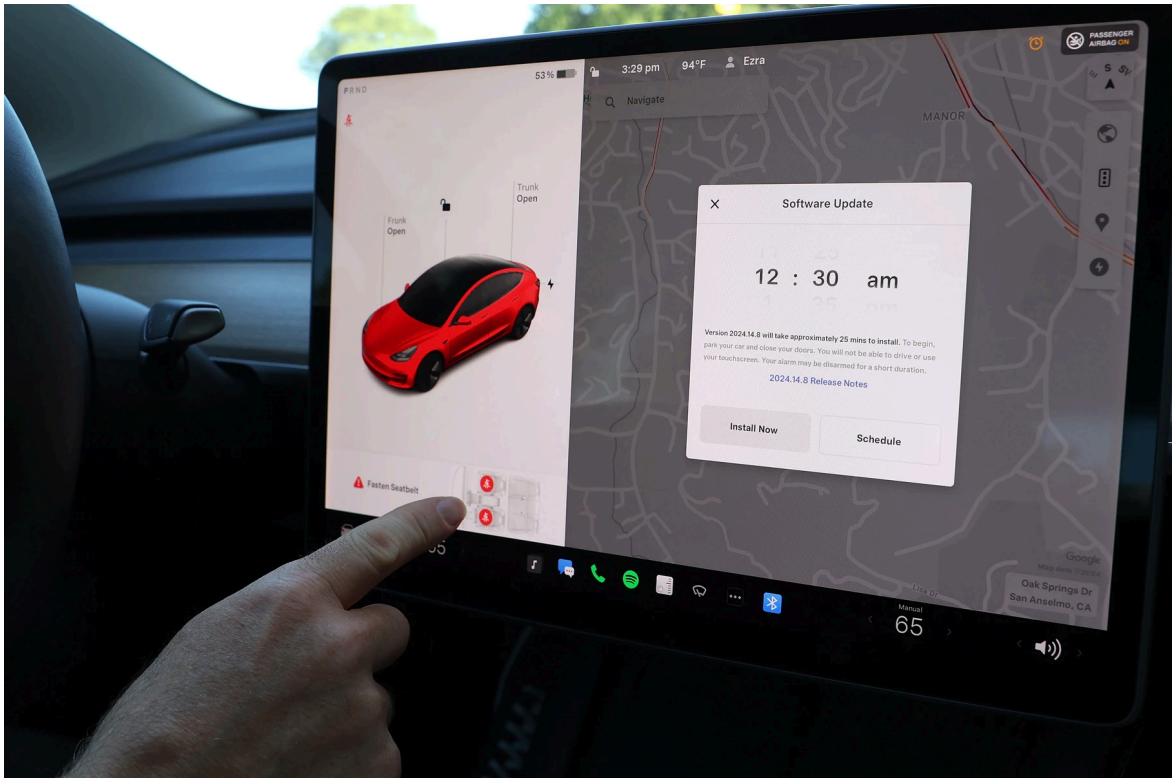
Donahue with the National Sheriffs’ Association agrees that the cameras are “not to track the ordinary citizen going to the grocery store.”

“Obviously, we’re going to protect the Fourth Amendment,” he added.

Inside Your Smart Car

General Motors Co. brought one of the first connected car features to the US market in the late 1990s, with OnStar, an in-vehicle security and emergency services feature. But now cars can read aloud texts, call family members on voice command, and suggest destinations, all information that can be traced. And they can scan faces with driver-facing cameras, collect listening habits and purchasing choices, and gather driving and braking data that can be used by insurers and police.

Drivers relinquish many rights to that personal information when they buy or rent a vehicle, the permissions often buried in fine print.



A software update alert appears on the screen of a Tesla Model 3 on May 31, 2024, in San Anselmo, Calif. Photographer: Justin Sullivan/Getty Images

Three states and class action plaintiffs have sued General Motors and other automakers, accusing them of sharing precise geolocation and driver behavior data collected by OnStar without getting clear consent from consumers. GM has stopped the data sharing with data brokers, and also reached a

settlement with the Federal Trade Commission, but state litigation is still pending.

Privacy experts and some lawyers say rulings like *Carroll* and *Knotts* don't work when cars have become extensions of smart phones and cameras can trace every move of ordinary citizens.

"If you physically have your hands on a car, good for you, because you essentially have an unlocked phone," said Eleni Manis, research director at the Surveillance Technology Oversight Project, a New York-based privacy group.

While the Supreme Court hasn't revisited the Fourth Amendment and how it applies to emerging technologies since *Carpenter,* attorneys fighting police over license plate readers say lower courts could provide some answers. The Norfolk case is scheduled for trial Oct. 7, and the Institute for Justice plans to appeal the case to the Fourth Circuit if it loses.

A federal judge dismissed the Illinois case on March 31, finding that plaintiffs failed to show they have been or will be investigated because of information obtained via the license plate readers. The judge didn't address whether a more extensive network of license plate readers might infringe a reasonable expectation of privacy.

Attorneys at Liberty Justice Center are evaluating whether to amend their lawsuit or appeal.

"We're saying we think this is well over the line, and we think that this is a place to try and take a stand," Stephens said. "It's time to create standards for the 21st century, and time to make the Fourth Amendment work for these new technologies."

To contact the reporters on this story: Cassandre Coyer in Washington at ccoyer@bloombergindustry.com; Tonya Riley in Washington at triley@bloombergindustry.com; Jorja Siemons in Washington at jsiemons@bloombergindustry.com

To contact the editors responsible for this story: Gregory Henderson at ghenderson@bloombergindustry.com; Kartikay Mehrotra at kmehrotra@bloombergindustry.com