



INSTITUTE FOR JUSTICE

Written Testimony of Alasdair Whitney
Legislative Counsel, The Institute for Justice
Before the U.S. Senate Subcommittee on Crime and Counterterrorism
September 23, 2026
Always Watching: Flock's Nationwide AI Surveillance Network

Dear Chairman Hawley, Ranking Member Durbin, and Members of the Subcommittee:

Thank you for the opportunity to testify before the Subcommittee. My name is Alasdair Whitney, and I am Legislative Counsel at the Institute for Justice (IJ). IJ is a nonprofit, nonpartisan public interest law firm that works around the country to defend constitutional rights. Through IJ's Project on the Fourth Amendment and our Plate Privacy Project, we have challenged the unconstitutional use of automatic license plate readers (ALPRs) to collect vast troves of data on ordinary people's movements through litigation, legislative advocacy, and grassroots organizing. We commend the Subcommittee for convening this hearing, and we commend the Chairman for opening an investigation into these AI-powered surveillance camera networks.

ALPR technology now lets the government do something it could never do before: travel back in time and reconstruct where you went, whom you saw, and what you did over weeks or even months. Agents can do this as easily as running a Google search. What they almost never have to do is ask for a judge's permission before pulling up a month of someone's movements. Governments say they need that kind of frictionless access to fight crime, and the goal is, of course, a commendable one. But convenience and oversight have always pulled in opposite directions, and the Fourth Amendment resolves that tension in favor of oversight. Fifty-five years ago, before any of this technology existed, the Supreme Court rejected the argument that efficiency alone could excuse the government from asking a judge first. The warrant requirement, it held in *Coolidge v. New Hampshire*, is "not an inconvenience to be somehow 'weighed' against the claims of police efficiency."¹ Technology may make surveillance more convenient, but it does not make the Fourth Amendment less important.

What ALPRs Have Become

Modern ALPRs photograph nearly every car that passes them. Unlike an officer posted at an intersection, they do not blink, take breaks, or sleep. They run around the clock and can capture images of vehicles traveling at highway speeds and in the dark.² Every capture creates a record of a location and a time, and that record goes into a searchable database.

These surveillance platforms capture far more than a license plate number. The market leader, Flock Safety, uses artificial intelligence to convert each vehicle's visual features—make, model,

¹ 403 U.S. 443, 481 (1971).

² Complaint ¶¶ 19–22, *Schmidt v. City of Norfolk*, No. 2:24-cv-621 (E.D. Va. Oct. 21, 2024), ECF No. 1 [hereinafter *Norfolk Compl.*]; Complaint ¶¶ 20–23, *Tan v. City of San Jose*, No. 5:26-cv-03181 (N.D. Cal. Apr. 15, 2026), ECF No. 1 [hereinafter *San Jose Compl.*]; Pls.' Mem. in Supp. of Mot. for Partial Summ. J. at 3, *Schmidt v. City of Norfolk*, No. 2:24-cv-621 (E.D. Va. Nov. 20, 2025), ECF No. 179-1 (Statement of Undisputed Material Facts) [hereinafter *Norfolk SJ Mem.*].

color, bumper stickers, roof racks, dents—into what it markets as a searchable “Vehicle Fingerprint.”³ An officer can search for a full or partial plate, filter by those features, or type a description like “blue Mustang with racing stripes.” With a few more clicks, the officer can generate a “Vehicle Journey Map” showing everywhere a car has been captured, run “convoy analysis” to identify vehicles frequently seen together, list every vehicle that visited a set of locations, and try predict where a car is likely to go next.⁴ Flock is working tirelessly to enhance those capabilities. For instance, Wired reporters reconstructed Flock’s code to reveal that it was rolling out new AI tools that would allow officers to quickly and effortlessly reconstruct people’s routes over extended time periods and compile lists of their likely associates.⁵

Perhaps the most valuable feature of this surveillance architecture is its network effect. Agencies pool their data into a multijurisdictional database that tracks a person’s movements across cities, states, and the entire country, so an officer in California or Texas has the power to see where a motorist has traveled in Missouri or Illinois. Flock alone now operates more than 120,000 cameras in 49 states and logs more than 20 billion vehicle scans a month.⁶ These cameras sit in front of doctors’ and attorneys’ offices, places of worship, hospitals, military installations, even homes.⁷ And the volume is staggering. San Jose’s ALPR network, which numbers 474 cameras, collected over 360 million photographs in 2024; approximately one-quarter of one percent triggered a hotlist alert.⁸ Norfolk’s 175 cameras logged more than 41 million vehicle captures in a single 29-day period; fewer than two percent of detections trigger any alert at all.⁹ Norfolk’s chief of police remarked that “[i]t would be difficult to drive anywhere of any distance without running into a camera somewhere.”¹⁰

These capabilities are exactly why law enforcement likes this technology. As the Supreme Court put it in *Carpenter v. United States*, location records provide “an intimate window into a person’s life.”¹¹ Through that window, the government can see or infer whether you attend church or a mosque, whether you visit a doctor, a therapist, an immigration lawyer, a union hall, a protest, or a gun range. And although the databases do not typically include names, an officer can look up a plate’s registered owner in seconds and pull addresses, relatives, and associates from other government databases.¹² What emerges is not a glimpse of a day in the life but an unblinking stare into a way of life.

A Technology With Few Rules

Concerningly, there is no federal statute governing how ALPR data is collected, accessed, secured, retained, or shared. Nor has Congress attached any meaningful ALPR-related

³ San Jose Compl. ¶¶ 32–34.

⁴ *Id.* ¶¶ 34–35; Norfolk SJ Mem. at 3–4.

⁵ Dhruv Mehrotra & Dell Cameron, *Flock Has a Powerful New AI Tool for Police. We Got Its Code*, Wired (Aug. 19, 2026), <https://www.wired.com/story/flock-safety-os-investigate/>.

⁶ Letter from Sen. Josh Hawley, Chairman, Subcomm. on Crime & Counterterrorism, to Garrett Langley, CEO, Flock Safety (Aug. 26, 2026), <https://www.hawley.senate.gov/chairman-hawley-investigates-ai-powered-flock-cameras-amidst-privacy-concerns/> [hereinafter Hawley Letter].

⁷ See San Jose Compl. ¶ 48 & figs. 4–7; Norfolk Compl. ¶¶ 53–55.

⁸ San Jose Compl. ¶ 47.

⁹ Norfolk SJ Mem. at 11, 22.

¹⁰ *Id.* at 8 (citation omitted).

¹¹ 585 U.S. 296, 311 (2018).

¹² San Jose Compl. ¶¶ 27–28, 53.

conditions to the federal grant dollars that buy these cameras, even though, as the Congressional Research Service notes, JAG and COPS funds have paid for license plate reader programs around the country.¹³ About half the states do not regulate this technology either.¹⁴ Where retention limits exist, they run from three minutes in New Hampshire to five years in Alabama.¹⁵ Minnesota has the nation’s strongest warrant requirement, yet because it applies only to “monitor[ing] or track[ing]” someone who is “the subject of an active criminal investigation,” it protects suspects while appearing to leave innocent drivers entirely unprotected.¹⁶

Even where states have acted, the reforms have not gone far enough. Virginia’s 2025 law is the best example of an inchoate effort. It capped retention at 21 days and prohibited sharing with out-of-state and federal agencies but did not impose a warrant requirement and relies on the agencies themselves to comply.¹⁷ Predictably, compliance has been inconsistent. The Virginia State Crime Commission surveyed all 361 law enforcement agencies in the Commonwealth a few months after the law took effect. Nearly a third did not respond at all. Of the 159 that did and reported using ALPRs, many openly acknowledged noncompliance:¹⁸

- Twenty-one percent (33 agencies) had kept data longer than 21 days;
- Thirty agencies had given access to federal or out-of-state agencies;
- Sixteen percent had no ALPR policy at all, which is required under the law, and another nine percent were still drafting one; and
- Thirty-five percent had never notified the public of ALPR use, although the statute requires it.

The City of Norfolk, Virginia, shows how a retention-only rule leaks even when an agency follows it. The city reads the 21-day limit as inapplicable to data that officers download, so an officer can pull data for a permitted purpose and keep it indefinitely on a rolling basis.¹⁹

Where governments have not written the rules, a vendor or law enforcement agency has. Many agencies never make an independent decision about how long to keep plate data and instead simply adopt whatever their vendor’s software is set to do. Flock, facing public backlash, revised its default retention period from 30 days to seven and made its audit tools mandatory, but

¹³ Cong. Rsch. Serv., R48160, *Law Enforcement and Technology: Use of Automated License Plate Readers*, <https://www.congress.gov/crs-product/R48160> (last visited Sept. 19, 2026).

¹⁴ See Legis. Analysis & Pub. Pol’y Ass’n, *Automatic License Plate Recognition Systems: Summary of State Laws*, <https://legislativeanalysis.org/wp-content/uploads/2025/09/Automatic-License-Plate-Recognition-Systems-Summary-of-State-Laws.pdf> (last updated Sept. 2025).

¹⁵ Compare N.H. Rev. Stat. Ann. § 261:75-b, with Ala. Admin. Code r. 265-X-6-.06 (five-year maximum, set by rule rather than statute).

¹⁶ Minn. Stat. § 13.824, subd. 2(d).

¹⁷ Va. Code Ann. § 2.2-5517.

¹⁸ Va. State Crime Comm’n, *Law Enforcement Use of Automatic License Plate Recognition (ALPR) Update*, in 2025 *Annual Report* (Jan. 2026), <https://vscc.virginia.gov/Annual%20Reports/2025%20VSCC%20Annual%20Report%20-%20Law%20Enforcement%20Use%20of%20ALPR%20Update.pdf>.

¹⁹ Br. of Appellants at 12–13, *Schmidt v. City of Norfolk*, No. 26-1227 (4th Cir. Apr. 13, 2026), ECF No. 16 [hereinafter Appellants’ Br.].

those changes do not go nearly far enough.²⁰ Even if they came close, many of the optional “rules” suggesting how law enforcement accesses drivers’ historical location information are, today, whatever one company decides they should be this quarter.

Predictable Misuse and Abuse

Because there is no warrant requirement gatekeeping access to ALPR databases, misuse and abuse of the technology are the predictable products of the system’s design. IJ’s Database of ALPR Abuse now catalogs more than 240 incidents nationwide, and the categories are disturbingly consistent.²¹

In August, for example, the Washington Post published a nationwide review of police and court records. It identified dozens of officers charged with or accused of using license plate readers for unauthorized purposes. These officers used Flock’s system in 46 of those cases, and in 26 the targets were officers’ current or former partners, their exes’ new partners, or women the officers wanted to meet.²² One of them was Marci Bakely, a single mother in Jefferson, Georgia, who could not understand how her ex-boyfriend always seemed to know where she was. He was the police chief of a nearby town, and audit logs show he searched her plate and her teenage daughter’s roughly 600 times before his arrest last November on stalking and harassment charges.²³ In Milwaukee, Officer Josue Ayala ran his partner’s plate 124 times and her ex-boyfriend’s 55 times, typing “investigation” as his reason each time.²⁴ A private citizen only learned of this when looking up his own plate on a public website that republishes agency search logs.²⁵ Months later, one of the internal affairs detectives assigned to investigate Ayala was himself charged with improperly using Flock to track two people, logging his searches as “training” and “test.”²⁶

Then there is the category of misuse that makes other abuse possible: searching for no reason, or with a reason so vague that no supervisor, auditor, or judge could ever tell what the officer was actually looking for. Norfolk’s data was searched more than 230,000 times between May 2023 and mid-2025.²⁷ The three most common stated reasons were “cj,” “stolen,” and “inv,” which together accounted for nearly 75,000 searches.²⁸ One officer repeatedly logged “protestor identification” and another repeatedly typed “la la la la.”²⁹ No one audited these hundreds of thousands of searches until our lawsuit forced the city to do so in February 2025. Unfortunately,

²⁰ Drew Harwell, Douglas MacMillan & Aaron Schaffer, *Flock Unveils Changes After Post Report on Police Misuse of Camera Network*, Wash. Post (Aug. 13, 2026), <https://www.washingtonpost.com/technology/2026/08/13/flock-unveils-changes-after-post-report-police-misuse-its-network/>.

²¹ Inst. for Just., *The IJ Database of ALPR Abuse*, <https://ij.org/the-ij-database-of-alpr-abuse/> (last visited Sept. 20, 2026).

²² Drew Harwell, Douglas MacMillan & Aaron Schaffer, *How Rogue Officers Turned a Nationwide Camera Network into a Tool for Stalking*, Wash. Post (Aug. 2, 2026), <https://www.washingtonpost.com/technology/2026/08/02/how-police-officers-used-vast-network-cameras-spy-their-exes/>.

²³ *Id.*

²⁴ Eric Levenson, *Inside the Growing Police Use and Misuse of Flock’s License-Plate Reader Cameras*, CNN (July 26, 2026), <https://www.cnn.com/2026/07/26/us/flock-cameras-surveillance-abuse>.

²⁵ Hawley Letter, *supra* note 6.

²⁶ Levenson, *supra* note 24.

²⁷ Norfolk SJ Mem. at 13.

²⁸ *Id.*

²⁹ *Id.*

these practices are not unusual. A Lake County, Indiana sheriff's deputy searched more than 19,000 cameras in 1,558 cities and towns; his reason was "LMAO."³⁰ And once journalists began mining these logs, officers were told to be "as vague as permissible."³¹

Even when officers act in good faith, a single misread character or other technology-related error can put innocent people at gunpoint. IJ has documented at least 33 cases since 2018, most of them since 2023, in which innocent motorists were stopped, detained, or jailed because of ALPR errors. In Sherwood, Arkansas, this February, a one-letter misread led officers to pull a couple out of their SUV at gunpoint and handcuff them while their one-month-old baby sat in the back seat.³² In Roseville, California, the police department reviewed the 1,427 stolen-vehicle and felony alerts the Flock system sent it over two years and found the cameras had misread the plate in 71 percent of them.³³ In one week alone, a supervisor told Flock that 16 of the 17 plates it had flagged were wrong, some of them, in her words, "blatant misreads."³⁴

Finally, there is the related question of where all the troves of data end up. Last December, Flock accidentally exposed internal training materials showing that it was sending images of people and vehicles from its U.S. cameras to gig workers in the Philippines, hired through an online freelancing platform, to annotate the images and train its artificial intelligence.³⁵ And last week, hackers who pulled a Flock camera off a pole reported that they had copied its storage, recovered an encryption key the company had left on the device itself, and accessed roughly three weeks of footage showing some 50,000 vehicles.³⁶ Consider what that means in a city like Norfolk, home to some of the largest naval installations on earth. A record of where sailors, officers, and their families drive each day, who they meet, and when they leave the base is exactly the kind of record a foreign intelligence service would pay for. A database of everyone's movements is not just a privacy problem. It is also a target for bad actors.

What We Found in Norfolk and San Jose

The Supreme Court has said repeatedly that Americans do not surrender their privacy when they back out of the driveway or go about their day in public. In *Carpenter*, for instance, the Court held that "individuals have a reasonable expectation of privacy in the whole of their physical movements" and required a warrant for seven days of cell-site records, which are far less precise

³⁰ Jason Koebler, *Cops Search Thousands of Flock Cameras for Reasons of 'LMAO,' 'IDK,' 'Hehe,' and 'asdfg'*, 404 Media (Sept. 14, 2026), <https://www.404media.co/cops-search-thousands-of-flock-cameras-for-reasons-of-lmao-idk-hehe-and-asdfg/>.

³¹ *Id.*

³² Inst. for Just., *Dozens of Innocent Motorists Have Been Pulled Over, Detained at Gunpoint, or Jailed Due to AI License Plate Camera Errors* (July 1, 2026), <https://ij.org/dozens-of-innocent-motorists-have-been-pulled-over-detained-at-gunpoint-or-jailed-due-to-ai-license-plate-camera-errors/>.

³³ Nicole Einbinder, *In One California Town, Flock Misread License Plates in 71% of the Alerts It Sent to Police*, Bus. Insider (July 31, 2026), <https://www.businessinsider.com/flock-camera-misread-license-plate-reader-california-roseville-police-2026-7>.

³⁴ *Id.*

³⁵ Joseph Cox, *Flock Uses Overseas Gig Workers to Build Its Surveillance AI*, 404 Media (Dec. 1, 2025), <https://www.404media.co/flock-uses-overseas-gig-workers-to-build-its-surveillance-ai/>.

³⁶ Joseph Cox & Dhruv Mehrotra, *Hackers Stole Flock's Camera Software, Revealing How the Company Tracks Cars and People*, 404 Media (Sept. 16, 2026), <https://www.404media.co/hackers-stole-flocks-camera-software-revealing-how-the-company-tracks-cars-and-people-2/>.

than an ALPR capture.³⁷ The en banc Fourth Circuit then held that Baltimore’s limited aerial surveillance program, which captured people and cars as “blurred dots or blobs” and retained those images for 45 days, was a search because it created “a retrospective database of everyone’s movements across the city.”³⁸ And this June, in *Chatrie v. United States*, the Court held that police invaded a reasonable expectation of privacy by obtaining “only two hours” of a suspect’s location history from Google.³⁹ The Court refused to treat the quantity of data as dispositive, and instead focused on what the technology is capable of revealing, not merely what law enforcement happened to find.⁴⁰ *Chatrie* is not an ALPR case, but it dismantles the industry’s favorite defense, which is that a limited window of data held by a vendor is nothing to worry about. And as *Chatrie* confirms, even short-term monitoring can reveal a trip to a church, a clinic, or a lawyer’s office.⁴¹

IJ is litigating the application of this caselaw to ALPRs, and discovery has shown what an ALPR dragnet actually looks like. In October 2024, we sued Norfolk, Virginia, on behalf of Lee Schmidt, a Navy veteran with 21 years of service, and Crystal Arrington, a certified nursing assistant who drives elderly clients to appointments in Norfolk nearly every day. Neither has been charged with a crime.⁴² With Flock’s help, Norfolk strategically positioned its cameras to maximize the data they collect and prevent routes around them.⁴³ An expert witness, a professor of applied mathematics, modeled more than 15,000 representative driving routes and found that cameras generated data on virtually every route.⁴⁴ In less than five months, Flock cameras in the area logged Lee’s plate at least 526 times and Crystal’s at least 849 times.⁴⁵ To try and replicate this surveillance the old-fashioned way, Norfolk would need at least 352 officers, about 70 percent of its department, working twelve-hour shifts, seven days a week.⁴⁶

On January 27, 2026, the district court granted summary judgment to the city. It read *Carpenter* to mean that surveillance becomes a search only when it “crosses the line into cataloging the whole, or nearly the whole, of a person’s movements” and concluded that Norfolk’s cameras fell short because they captured drivers only at fixed points, with gaps in between.⁴⁷ *Chatrie* has since rejected exactly that kind of quantitative threshold.⁴⁸ We have appealed, and the case is fully briefed in the Fourth Circuit, which is poised to be one of the first federal appellate courts to apply *Chatrie* to an ALPR network.⁴⁹

Here is the part that matters most for this Subcommittee. The court acknowledged that ALPR surveillance “could become too intrusive and run afoul of” constitutional privacy standards “at

³⁷ 585 U.S. at 310 & n.3, 312.

³⁸ *Leaders of a Beautiful Struggle v. Balt. Police Dep’t*, 2 F.4th 330, 334, 345 (4th Cir. 2021) (en banc).

³⁹ *Chatrie v. United States*, 146 S. Ct. 2193, 2211, 2215 (2026).

⁴⁰ *Id.* at 2210 & n.9, 2211.

⁴¹ *See id.* at 2202, 2208.

⁴² Norfolk Compl. ¶¶ 51–73.

⁴³ Norfolk SJ Mem. at 5–6.

⁴⁴ Appellants’ Br. at 17–19.

⁴⁵ Appellants’ Br. at 15–16.

⁴⁶ Norfolk SJ Mem. at 25.

⁴⁷ *Schmidt v. City of Norfolk*, 819 F. Supp. 3d 492, 511 (E.D. Va. 2026); *see* Appellants’ Br. at 16.

⁴⁸ *Chatrie*, 146 S. Ct. at 2210 n.9.

⁴⁹ *Schmidt v. City of Norfolk*, No. 26-1227 (4th Cir. docketed Feb. 26, 2026).

some point,” and it said that experimentation with this technology “is best achieved with input from the public and with guardrails erected by state legislatures or local governing bodies.”⁵⁰

San Jose is where this technology is heading and shows why legislative action is necessary. In 2021, the city had four Flock cameras at one intersection; today it has 474.⁵¹ This network is capable of capturing more than 360 million photographs a year.⁵² More than 1,000 city employees have access to the data, and it is shared with nearly 300 other government entities.⁵³ Between July 1 and December 9, 2025, San Jose’s data were searched nearly 2.5 million times, which is an average of more than 15,000 searches a day, with no warrant.⁵⁴ And although California law prohibits sharing this data with out-of-state agencies, records show California agencies ran searches on behalf of federal agencies in at least 20 cases, with more than a dozen other searches listing “ICE,” “CBP,” or “HSI” as the reason.⁵⁵

The Solution: Require a Warrant

The Fourth Amendment sets a floor, not a ceiling, and Congress has gone beyond it repeatedly and without controversy for wiretaps⁵⁶ and bank records.⁵⁷ A statute requiring a warrant before the government mines a database of people’s movements is no different in kind.

IJ’s model legislation, the Protecting Everyone from Excessive Police Surveillance (PEEPS) Act, is appended to this letter. It requires a government official to obtain a warrant before accessing historical location information—data more than two hours old—from any database, public or private, that can reveal where a person or vehicle has been. Its exceptions to the warrant requirement track the Fourth Amendment’s own, and it leaves toll, traffic, and parking enforcement alone. Data less than two hours old stays available on a reasonable suspicion of a felony, in emergencies, and through hotlist alerts, which is how, for example, stolen cars and missing children are usually found. Two hours is where the Act separates roughly contemporaneous location information from historical location information. It is a principled drafting line rather than a constitutional floor; indeed, in *Chatrie*, the Supreme Court found a search in just two hours of location history.⁵⁸ It also bars sharing across jurisdictions without a court order and bars any sale. It requires a record of every access, employee supervisor audits every 30 days, and an annual public report. Importantly, it caps data retention at seven days absent a warrant, and it makes evidence obtained in violation of the Act inadmissible.

What the Act does not do matters just as much: it does not ban a single camera, limit hotlist alerts, or prevent officers from using the technology to respond to emergency situations. It simply puts a neutral judge between the government and the past movements of people who have done nothing wrong. Law enforcement officers are familiar with this process. They obtain

⁵⁰ *Schmidt*, 819 F. Supp. 3d at 497–98.

⁵¹ San Jose Compl. ¶¶ 41, 46.

⁵² *Id.* ¶ 47.

⁵³ *Id.* ¶¶ 1, 58.

⁵⁴ *Id.* ¶ 69.

⁵⁵ *Id.* ¶ 70.

⁵⁶ 18 U.S.C. §§ 2510 *et seq.*

⁵⁷ 12 U.S.C. §§ 3401 *et seq.*

⁵⁸ *Chatrie*, 146 S. Ct. at 2215.

warrants every day to tap phones and pull cell-site location records. Adding license plate data to that list asks nothing of law enforcement it has not done routinely for decades.

Congress has tools no state does, and we respectfully urge the honorable members of this Subcommittee to use them. Bind federal officials to a warrant requirement for historical location information and close the “side door” through which federal agents ask local officers to run searches they could not run themselves. And condition federal grant money on states or localities adopting PEEPS-level safeguards; DHS already conditions some funding on the existence of an ALPR policy, and Congress can specify what that policy must contain.⁵⁹

Every time the federal government funds and expands this technology without rules, it answers a fundamental question: should the government be able to track your every move without a warrant? So far, by its silence, the answer seems to be yes. It does not have to be. These systems do not show a day in the life. They show a way of life. As the Supreme Court put it in June, this technology is “new, but the principle covering it is not.”⁶⁰ We respectfully urge Congress to err on the side of the Constitution and to require a warrant before the government reaches back through Americans’ location histories and before these cameras end up on every street corner.

Thank you again for the opportunity to testify.

Respectfully submitted,

Alasdair Whitney
Legislative Counsel
Institute for Justice
901 North Glebe Road, Suite 900
Arlington, Virginia 22203
awhitney@ij.org
www.ij.org

⁵⁹ Cong. Rsch. Serv., *supra* note 13.

⁶⁰ *Chatrpie*, 146 S. Ct. at 2217.

APPENDIX

The Protecting Everyone from Excessive Police Surveillance (PEEPS) Act

Model Legislation

August 2025

Revised in September 2026

Section 1. Short Title.

This Act may be cited as the PEEPS Act.

Section 2. Legislative Findings and Purpose.

The legislature finds that government officials or government entities violate individuals' right to privacy, and the constitutional principles that protect it, when, without adequate safeguards, they use technology to create, access, or share data that reveal, or can be used to reveal, individuals' or vehicles' location information. This Act regulates the access to, sharing of, retention of, and security of that information.

Section 3. Definitions.

For purposes of this Act:

“Access” means viewing, querying, retrieving, copying, transmitting, analyzing, downloading, or otherwise using a database, whether manually or automatically.

“Collect” means using technology, including but not limited to license plate readers, cameras, sensors, or aerial drones, to record information about the physical locations, movements, or movement patterns of individuals or vehicles.

“Contemporaneous location information” means data that, when accessed, reveals the location or locations of individuals or vehicles less than two hours before the time of the access.

“Database” means a physical or digital information storage system, whether publicly or privately owned, that contains location information in any form, including but not limited to photographs, video, audio recordings, license plate data, facial recognition data, cell site location information, device signal data, or any combination, index, or analysis of these.

“Government entity” means any government agency, office, bureau, division, board, council, commission, or political subdivision.

“Government official” means any officer, employee, agent, contractor, or representative of a government entity.

“Historical location information” means data that, when accessed, reveals the locations of individuals or vehicles more than two hours before the time of the access.

“Hotlist” means a list of license plate numbers or other unique identifiers that is compared, automatically or manually, against contemporaneous location information as it is collected, for the purpose of generating an alert when a match occurs.

“Location information” means contemporaneous location information and historical location information. The term does not include:

- a. audio, video, or photographic recordings, including recordings captured by a camera in a government-owned building, a body-worn camera worn by an on-duty government official, or a dashboard camera installed in or on a vehicle owned by a government entity, that satisfy both of the following:
 1. the recordings have not been processed or indexed to identify, classify, match, reidentify, track, or reconstruct movements of a particular individual or vehicle, other than an on-duty government official or a government-owned vehicle; and
 2. the recordings have not been networked, pooled, combined, or otherwise organized with other recordings or data in a manner that readily permits a government official to search across multiple locations for an individual, vehicle, or group of individuals or vehicles or to reconstruct movements across those locations;
- b. information generated by a device worn or carried by an individual pursuant to a court order or a condition of pretrial release, probation, parole, or other individualized supervision;
- c. records created or maintained for administrative or recordkeeping purposes, rather than to track or reconstruct the movements of individuals or vehicles, including property, tax, vital, business- and professional-licensing, voter-registration, 9-1-1 and emergency-dispatch, and court records; and
- d. information that reveals only an address of residence, ownership, or registration, and not the presence of a particular individual or vehicle at a particular time.

“Supervisor” means a government official who has the authority to direct and discipline several government officials within a government entity.

“Warrant” means a court order that meets the requirements of the Fourth Amendment’s warrant clause. For purposes of this Act, a subpoena is not a warrant.

Section 4. Location Information Access.

- a. A government official may not access historical location information unless one or more of the following exceptions apply:
 1. the government official has obtained a warrant to access the database;
 2. each individual whose historical location information would be revealed expressly consents, so long as that consent does not allow the government official to access the historical location information of individuals who have not expressly consented;
 3. the registered owner of a vehicle reports the vehicle lost or stolen and expressly consents;
 4. exigent circumstances make it impractical to obtain a warrant before the exigency expires; or
 5. the government official is carrying out one or more of the following purposes and uses the historical location information solely for those purposes:
 - i. apprehending an individual for whom there is an outstanding arrest warrant, provided that the offense for which the warrant was issued would be a felony under the laws of this state;
 - ii. toll collection and enforcement, provided that the access is limited to a specific toll or fare transaction or violation and does not reveal the individual's or vehicle's location at any other time;
 - iii. traffic enforcement, provided that the access is limited to a specific traffic violation and does not reveal the individual's or vehicle's location at any other time;
 - iv. parking enforcement, provided that the access is limited to a specific parking violation and does not reveal the individual's or vehicle's location at any other time; or
 - v. information security, as necessary to implement the requirements of section 5.
- b. A government official may not access contemporaneous location information unless one or more of the following exceptions apply:
 1. an exception listed in subsection (a) applies, applied as though each reference in that subsection to historical location information were a reference to contemporaneous location information;

2. the government official has a reasonable suspicion that the individual or vehicle whose location would be revealed by the access has committed, is committing, or is about to commit an offense that would be a felony under the laws of this state;
3. the government official has an objectively reasonable basis to believe that the access is necessary to prevent imminent harm to a person or imminent substantial damage to property; or
4. the access consists solely of the comparison of contemporaneous location information against a hotlist and the receipt or review of any alert generated by that comparison, provided that the access is limited to the contemporaneous location information produced by the single collection that generated the alert.

Section 5. Location Information Security.

- a. A government official or government entity that collects location information may not share it outside the official's or entity's jurisdiction, except for a reason set forth in section 4 or pursuant to a valid court order. For purposes of this Act, a subpoena is not a valid court order.
- b. A government official or government entity that collects location information may not sell or convey it to a private, nongovernmental third party for any reason, whether as a market transaction, a response to a public records request, or otherwise. This subsection does not prohibit a government official or government entity from conveying location information to a vendor that operates the database on the official's or entity's behalf, solely as necessary for the vendor to correct errors or defects in, or to secure, the database, software system, or related technology.
- c. A government official or government entity that collects location information shall adopt a policy for compliance with this Act. The policy shall:
 1. ensure that the security and access requirements of this Act are being followed;
 2. ensure that location information is encrypted or otherwise rendered unreadable to an unauthorized person using methodology or technology generally accepted in the field of information security;
 3. ensure that government officials do not access a database that reveals location information absent a showing to a supervisor, and written approval by that supervisor, that the access complies with section 4(a);
 4. ensure that a record is created and maintained every time location information is accessed, which record shall include:
 - i. the identity of the government official and government entity;

- ii. the specific purpose for such access;
 - iii. the provision of section 4 that permitted access and information sufficient to verify that the provision was satisfied;
 - iv. the written supervisor approval that granted access; and
 - v. the description of the location information accessed;
- 5. ensure that the records required under paragraph (4) of this subsection are audited by one or more supervisors not less frequently than every 30 days to ensure compliance with this Act. The government official or government entity shall create written standardized policies or practices for those audits that require, at a minimum:
 - i. verification that all information required under paragraph (4) of this subsection has been provided;
 - ii. verification that the specific purpose for which access was sought complies with this Act;
 - iii. verification that the scope of the location information accessed was appropriate in light of the specific purpose, including where the access is pursuant to a warrant, verification that the scope of the location information accessed is consistent with what the warrant permits;
 - iv. evaluation of whether any other factors suggest noncompliance with this Act, such as large volumes of searches by the same official, differing reasons for searching for similar location information, repeat searches of the same individual's or vehicle's location information without a warrant, or any other factors that would tend to suggest that the specific purpose provided for the search was pretextual or not permitted under this Act; and
 - v. if a supervisor conducting the audit determines or has reason to believe that a government official or government entity has violated any provision of this Act, further investigation of that actual or suspected violation;
- 6. ensure the creation and maintenance of an annual report that both compiles and summarizes the records described in paragraph (4) of this subsection, which report shall be made available to the legislature and the Governor on written request and to individuals pursuant to a valid public records request, provided that, before making the report available under this paragraph, the government official or entity shall redact from the report all personally identifiable information, including but not limited to license plate numbers and facial images; and

7. ensure that all government officials whose duties include accessing a database that contains location information complete training on how to comply with this Act and the compliance policy adopted pursuant to this subsection. The training may not be created or administered by a private entity whose business involves collecting location information.

Section 6. Retention of Location Information.

- a. Except as provided in subsection (b), a government official or government entity that collects location information may not retain the information for more than seven days after the date the information is collected.
- b. Location information that was accessed in compliance with section 4 may be retained for more than seven days only if:
 1. a valid judicial warrant or valid court order expressly authorizes the government official or government entity to retain the location information for more than seven days;
 2. the information is necessary to preserve evidence in an active criminal investigation, a supervisor makes a written determination, based on specific and articulable facts, that retaining the historical location information for more than seven days is required to apply for or obtain a warrant, and the information is not retained later than the 14th day after the date the information is collected; or
 3. an individual expressly consents to the retention of the individual's location information for more than seven days, and the consent complies with the requirements of section 4(a)(2) or (3).
- c. If a government official or government entity does not obtain a warrant to preserve location information retained under paragraph (2) of subsection (b) before the expiration of the period described in that paragraph, the official or entity shall permanently destroy the location information in accordance with subsection (d).
- d. On expiration of the applicable retention period under this section, the government official or government entity shall permanently destroy the location information and any copies of the information in a manner that renders the information unrecoverable.

Section 7. Enforcement Provisions.

- a. Location information accessed in violation of this Act is not admissible as evidence in any criminal, civil, or administrative proceeding.
- b. If a government entity learns that a government official within that government entity has violated any provision of this Act, the government entity shall suspend that government official's access to any database that contains location information:

1. for seven days upon a first violation;
 2. for 30 days upon a second violation; and
 3. permanently upon a third or subsequent violation.
- c. If the Attorney General has reason to believe that a government official or government entity has violated any provision of this Act, the Attorney General may bring a civil action for declaratory or injunctive relief to prevent any ongoing or future violations.
 - d. Nothing in this section precludes a government official or government entity from taking additional or more severe disciplinary action on learning of a violation of any provision of this Act.

Section 8. Local Regulation.

No municipality or other political subdivision of this state may enact an ordinance, regulation, or policy that allows government officials or government entities to access, retain, or share location information in a manner less restrictive than provided by this Act.