INSTITUTE FOR JUSTICE

February 23, 2026

Via Electronic Mail
200 E. Colfax Ave.
Denver, CO 80203

RE: Letter in Support of Senate Bill 26-070

Chair Weissman and Members of the Senate Judiciary Committee:

My name is Alasdair Whitney, and I am legislative counsel at the Institute for Justice (IJ), a national nonprofit organization dedicated to ending abuses of government power and securing constitutional rights. As part of our Project on the Fourth Amendment, we have challenged the unregulated and often unconstitutional use of automatic license plate readers (ALPRs) and the data those systems collect through litigation, legislation, and grassroots organization. We commend the committee for hearing this crucial piece of legislation and strongly urge your support.

Senate Bill 26-070 does not prohibit the use of ALPR technology. Rather, it puts limited but important guardrails in place so that this powerful surveillance technology is not abused. Specifically, this bill will create four commonsense safeguards: a warrant requirement to access historic location data (excluding exigencies), a limit on how long this data can be retained absent a legitimate reason, a prohibition on the sharing of this data outside of the jurisdiction in which it was collected without a warrant, and formal procedures for auditing the use of these systems. This ensures that law enforcement can benefit from these camera systems while also limiting the ability for the intimate data they create to be abused, misused, or compromised.

ALPRs have proliferated across the country in recent years. These cameras photograph every passing vehicle (not just those suspected of criminal activity) and use artificial intelligence to read the license plate and detect other distinctive features of vehicles (like the color, make, and even the presence of bumper stickers). This allows police to easily look up a vehicle and see where it has traveled. Unlike red light cameras or speeding cameras, these are not triggered by unlawful conduct but rather passively collect data on all motorists who pass by, feeding their information into a centralized, searchable database that can be accessed with little oversight. This data can be used to determine where, when, and with whom drivers travel, which can

901 N. Glebe Road, Suite 900 Arlington, VA 22203 P: (703) 682-9320 F: (703) 682-9321
general@ij.org www.ij.org

reveal highly intimate details about the lives of law-abiding motorists.

There are many vendors operating in this space, each with different capabilities and integrations. One vendor alone works with at least 5,000 law enforcement agencies across the country, offering access to a nationwide interconnected system which can be accessed and searched with minimal oversight.[1] The 112 ALPRs active in Denver captured over 2,184,000 vehicles in a 30-day period.[2] This is mass surveillance.

In late 2024, IJ filed a lawsuit on behalf of two individuals in Norfolk, Virginia, challenging the constitutionality of the city's 170-plus ALPR dragnet.[3] One of our clients had his vehicle tracked by the city's system 526 times in just a four-month period, validating the police chief's claim that it would be "difficult to drive anywhere of any distance without running into a camera somewhere."[4] Just last month, a judge ruled that the dragnet had not yet reached the point of violating the Fourth Amendment.[5] While disappointing, this ruling underscores the urgent need for legislators to step in and protect constitutional rights where the courts have failed.

Recently, headlines around the country have been splashed with stories detailing how this technology has been abused, misused, or compromised.[6] Many of these incidents have occurred right here in Colorado. From a Denver resident being falsely accused of stealing a package, to Loveland police providing access to their data to U.S. Border Patrol, to an

---

[1] Collier, K. (2025, November 1). *Police cameras track billions of license plates per month. Communities are pushing back*. NBC News. https://www.nbcnews.com/tech/tech-news/flock-police-cameras-scan-billions-month-sparking-protests-rcna230037

[2] Flock Safety. (n.d.). *Denver CO PD transparency portal*. Retrieved February 22, 2026, from https://transparency.flocksafety.com/denver-co-pd

[3] Institute for Justice. (n.d.). *Norfolk, VA Camera Surveillance*. https://ij.org/case/norfolk-virginia-camera-surveillance/

[4] Collier, K. (2025, September 8). *Police cameras tracked one driver 526 times in four months, lawsuit says.* NBC News. https://www.nbcnews.com/tech/security/virginia-police-used-flock-cameras-track-driver-safety-lawsuit-surveil-rcna230399; Brodkin, J. (2024, October 22). *Lawsuit: City cameras make it impossible to drive anywhere without being tracked*. Ars Technica. https://arstechnica.com/tech-policy/2024/10/lawsuit-city-cameras-make-it-impossible-to-drive-anywhere-without-being-tracked/

[5] Lee Schmidt and Crystal Arrington v. City of Norfolk, the Norfolk Police Department, and Mark Talbot, in his official capacity as the Norfolk Chief of Police. United States District Court Eastern District of Virginia Norfolk Division. Case 2:24-cv-00621-MSD-RJK. (2026). https://ij.org/wp-content/uploads/2026/01/Order-1-27-26.pdf

[6] For example, see: WSBTV.com News Staff. (2025, November 24). *New details: Former Braselton Police Chief accused of stalking; judge denied protective order.* WSB-TV. https://www.wsbtv.com/news/local/new-details-former-braselton-police-chief-accused-stalking-judge-denied-protective-order/DMECQENH7FGU5EQSD5XXUYZPYU/; Barrett, V. (2026, January 12). Menasha police officer accused of off-duty use of license plate tracking. *Post Crescent*. https://www.postcrescent.com/story/news/crime/2026/01/12/menasha-officer-cristian-morales-charged-with-misconduct-in-office/88142963007/; Koebler, J. (2025, August 12). *Feds used local cop's password to do immigration surveillance with Flock cameras.* 404 Media. https://www.404media.co/feds-used-local-cops-password-to-do-immigration-surveillance-with-flock-cameras/

Aurora family being pulled over at gunpoint because of an incorrect ALPR read (resulting in a $1.9 million settlement), examples of misuse and abuse abound close to home.[7]

In the absence of statewide regulations, some city officials are pushing back. Just last week, Denver Auditor Tim O'Brien refused to sign the city's contract with an ALPR vendor after Mayor Mike Johnson bypassed the city council to approve it. Noting data sharing as a concern, he explained, "I just want that data secure, so that you and I as citizens don't have our data being exposed to people that shouldn't have it[.]"[8] Concerns like Auditor O'Brien's are precisely what SB26-070 seeks to address.

The requirement that a government official obtain a judicial warrant prior to accessing historical location data is an essential safeguard against abuse. Warrants provide critical judicial oversight. And research has shown that warrants are typically granted quickly and generally approved on first submission.[9] While certainly not a perfect solution, it is one offered by our federal constitution to deter government abuse. Currently, there is no such safeguard in place.

Searches in response to exigent circumstances are exempt from the warrant requirement, ensuring that law enforcement will have access to potentially important data in a situation where getting a warrant would be impractical. Further, nothing in this law prohibits the use of "hotlists," which would be a key tool in an emergency.

By limiting the length of time jurisdictions may store data, this bill helps ensure that the day-to-day behavior of law-abiding Coloradans is not being stored for years in a database. Indeed, any database, no matter how secure, is at risk of being compromised. The Sheriff's Office of El Paso County—which is home to Army, Air Force, and Space Force installations—has 25 ALPRs, which scanned over 417,000 unique vehicles just last month.

---

[7] Prentzel, O. (2025, October 28). *After police used Flock cameras to accuse a Denver woman of theft, she had to prove her own innocence.* The Colorado Sun. https://coloradosun.com/2025/10/28/flock-camera-police-colorado-columbine-valley/; Soicher, S. (2025, August 15). *Loveland Police has shared access to license plate reader data with Border Patrol, records reveal.* 9News. https://www.9news.com/article/news/local/local-politics/loveland-police-sharing-license-plate-reader-data-border-patrol/73-807d8c95-5904-4b55-be83-27aafee9638d; Fichten, L., & Clark, A. (2025, July 24). *When license plate readers get it wrong.* CBS News. https://www.cbsnews.com/news/license-plate-readers-alpr-mistakes/

[8] Werthmann, K. (2026, February 19). *Denver auditor refuses to sign city's current contract with Flock Group: "I just want that data secure."* CBS News. https://www.cbsnews.com/colorado/news/denver-auditor-flock-cameras-contract/

[9] De Figueiredo, M. F., Hashimoto, B., & Thorley, D. (2025). Unwarranted warrants? An empirical analysis of judicial review in search and seizure. *Harvard Law Review*, *138*(8), 1959. https://harvardlawreview.org/print/vol-138/unwarranted-warrants-an-empirical-analysis-of-judicial-review-in-search-and-seizure/

Imagine how valuable this data would be in the hands of a foreign adversary or a criminal organization.

The restriction on interjurisdictional sharing is another crucial safeguard against not only abuse but violations of Colorado's existing ALPR regulations. While local Colorado law enforcement may take great pains to responsibly steward this data, without these restrictions, there is simply no way to guarantee that Colorado laws are respected and Colorado residents are safe from abuse when the data is accessed across state lines.

Finally, this bill requires that system use be regularly audited to ensure compliance with all the above provisions and others currently in law.

Together, these guardrails will greatly improve Coloradans' protections against warrantless mass surveillance. This bill creates a floor, ensuring jurisdictions that employ ALPR technology meet a minimum bar of responsibility and accountability. Colorado has an opportunity to lead the nation and set a standard for protecting individuals' reasonable expectation of privacy in the whole of their physical movements. This General Assembly should seize this opportunity before this technology proliferates further.

For these reasons, we strongly urge the committee to pass SB26-070. IJ stands ready to assist in the passage of this law, and we are happy to answer any questions you may have as you consider this legislation.

Respectfully,

Alasdair Whitney
Legislative Counsel
Institute for Justice
awhitney@ij.org

Post Office Box 975
100 Mikaela Way
Avon, CO 81620

February 20, 2026

Senate Judiciary Committee

SENT VIA E-MAIL:

Sen. Mike Weissman, Chair - mike.weissman.senate@coleg.gov
Sen. Dylan Roberts, Vice Chair - dylan.roberts.senate@coleg.gov
Sen. John Carson - john.carson.senate@coleg.gov
Sen. Lindsey Daugherty - lindsey.daugherty.senate@coleg.gov
Sen. Nick Hinrichsen - nick.hinrichsen.senate@coleg.gov
Sen. Katie Wallance - katie.wallace.senate@coleg.gov
Sen. Lynda Zamora Wilson - lynda.zamorawilson.senate@coleg.gov
Juliann Jenson - juliann.jenson@coleg.gov

Re: Senate Bill 26-070 Prohibiting a Government Entity from Accessing a Database that Stores Historical Location Information

Dear Senate Judiciary Committee members,

The Town of Avon installed Flock Safety license plate reader cameras several years ago. They have been instrumental in successfully responding to multi-jurisdictional crimes, including vehicle theft, burgleries, fraud, and fugitives in flight. Avon is often subject to criminal activity originating from outside of Eagle County due to our location on I-70.

Avon does not share this information with federal agencies or law enforcement agencies outside Colorado and does not share this information for commercial use. The ability to retain and access the license plate reader information for thirty (30) days without the need to obtain a warrant and the ability to share information with other law enforcement agencies within Colorado is important for effective, efficient and prompt response to criminal activity.

The Town of Avon highly values the privacy rights of our citizens. We have not experienced any instances of infringing on privacy of our citizens or any inappropriate use of license plate reader information since our deployment in Avon. We have experienced a meaningful improvement in our ability to respond to crime with the use of license plate reader technology.

Thank you for consideration of these comments.

Kind Regards,

Eric Heil, Town Manager

February 23rd, 2026

Senate Judiciary Committee
200 E Colfax Avenue
Denver, CO 80203

Testimony of Chrisanna Elser in Favor of SB26-070

Chair Weissman and Members of the Senate Judiciary Committee,

My name is Chrisanna Elser. I work in the financial industry—a sector where integrity is the only currency we have. In my world, an accusation of theft is a professional death sentence. But on September 27th, that identity was nearly dismantled not by a criminal, but by an Automatic License Plate Reader (ALPR) and an officer who treated its data as gospel. I was accused of a crime I never committed and was forced to prove myself innocent.[1] I am here to testify that this technology is being sold as a shield to protect communities, but in practice, it is a digital dragnet that turns our constitutional rights upside down.

Passing SB70 will help ensure that others will never have to go through what I endured. This bill creates many crucial guardrails to protect innocent Coloradans like me from the misuse and abuse of surveillance technology. For that reason, I urge you to support it.

When Sergeant Jamie Milliman of the Columbine Valley Police Department showed up at my door. I was informed that the department had a strong case against me for stealing a package from someone's home in Bow Mar. Why? Because an ALPR flagged my forest green Rivian entering and leaving Bow Mar. He told me, "You can't get a breath of fresh air in or out of that town without us knowing."[2] This is the fundamental danger of ALPR technology: it creates an illusion of omniscience that replaces police work with algorithmic arrogance.

He had a summons for theft ready before he even spoke to me. I was faced with the dystopian task of proving my innocence against the apparently incontrovertible evidence from the system.

As a result of this, I was subjected to two weeks of living hell.

I tried desperately to reach someone, anyone from Bow Mar or Columbine Valley who would listen. I started with the Columbine Valley police chief for a week, then moved up to town administrators, and finally the mayor of Bow Mar. I was passed around, ignored, and stonewalled for fourteen days.

---

[1] See: Prentzel, O. (28 October 2025). After police used Flock cameras to accuse a Denver woman of theft, she had to prove her own innocence. *The Colorado Sun.* https://coloradosun.com/2025/10/28/flock-camera-police-colorado-columbine-valley/.
[2] *Ibid.*

While these leaders were too busy to return my calls, the Columbine Valley Police Department was active on the Neighbors app, publicly posting my vehicle and soliciting "more evidence" from the public. They were crowd-sourcing a conviction for a crime I clearly did not commit, while the people in charge of the department refused to grant me five minutes of their time.

In the course of this investigation, what was said to the homeowner, my clients, or people in my social circles? In my industry, a whisper of "theft" can end one's career.

Thankfully, I was able to collect enough data about my whereabouts to prove I could not possibly have committed this crime. My husband and I had to spend our own money to build a digital "war chest" of GPS data and dashcam footage. When the chief of police finally looked at it, he sent a flippant email saying, "nicely done, btw" as if my exoneration was a school project and not the recovery of my life.

The most damning part is that the proof of my innocence was inside the very system they control. While the crime was occurring, my truck was parked directly in front of another Flock camera at my tailor's shop. The officer simply chose to ignore the timestamps and location data that didn't fit his narrative. He focused on an AI match of someone who looked "close enough" to the thief. If he had done his due diligence, I would have been exonerated in seconds.

This technology is extremely powerful. When misused or abused, it has the power to ruin someone's life. My story is proof.

I urge you to support SB26-070. No citizen should be forced into the impossible task of proving their innocence. The guardrails this bill puts in place will help ensure there is greater accountability in how these systems are used, how the information is maintained, and when it can be accessed. Without sensible legislation, stories like mine and others that have been in the news will continue to occur.

Don't let my nightmare become the standard for our state. Please pass SB26-070.

Respectfully,

Chrisanna Elser

Denver, Colorado

Written Testimony in Support of Senate Bill 26-070

The Protecting Everyone from Excessive Police Surveillance (PEEPS) Act

Colorado Senate Committee on Judiciary
Seventy-fifth General Assembly, Second Regular Session
February 23, 2026

Submitted by Justan Rice, Director of State Government Affairs, Libertas Institute

---

Mr. Chair and distinguished members of the Committee, thank you for the opportunity to testify in support of Senate Bill 26-070, the PEEPS Act. My name is Justan Rice, and I serve as Director of State Government Affairs at the Libertas Institute. Our work is rooted in a simple conviction: as technology advances, the fundamental liberties of every person should not retreat.

The Fourth Amendment in the Digital Age

The Fourth Amendment's guarantee is straightforward: the right of the people to be secure against unreasonable searches shall not be violated. In *Carpenter v. United States*, the Supreme Court confronted what that guarantee means in a world of pervasive digital surveillance. The Court's conclusion was clear: because digital location data creates a comprehensive record of a person's movements, accessing it constitutes a search.

Some will argue that there is no expectation of privacy in public spaces. But the Court drew a critical distinction—there is a vast constitutional difference between a passerby noticing you on a street corner and the government assembling a detailed, searchable log of everywhere you have been. The principle that government must demonstrate probable cause before tracking a person's movements does not weaken simply because surveillance technology has become cheaper and more convenient. SB 26-070 translates that constitutional principle into clear, enforceable Colorado law.

Addressing Operational Concerns

This bill is not anti-law enforcement—it is pro-Constitution. We take seriously the concerns raised about investigative speed, but it is important to distinguish between administrative convenience and constitutional necessity.

- **The 24-Hour Warrant Requirement.** Critics may suggest that requiring a warrant for data older than 24 hours creates an investigative bottleneck. In practice, telephonic and electronic warrants can be secured in minutes. This requirement is not a barrier to justice—it is a safeguard ensuring that a neutral magistrate, not a data broker, decides when a citizen's history is searched.
- **Data Retention Limits.** The bill's four-day retention limit prevents the state from becoming a permanent tracking agency for innocent people on the off chance they later become persons of interest. Once a warrant is obtained or a specific investigation is opened, data can be preserved indefinitely. The standard we are advocating is an "active investigation" standard—not a "perpetual dragnet."

Preserving Public Safety Tools

The PEEPS Act preserves every legitimate tool that officers need. The bill explicitly protects law enforcement's ability to act under exigent circumstances—kidnappings, active shooters, and other emergencies where time is of the essence. It does not slow the response to crises. What it does is prohibit the warrantless, suspicionless querying of commercial databases as a matter of routine—precisely the kind of general search the Fourth Amendment was written to prevent.

Accountability and Oversight

The bill also establishes meaningful transparency measures: supervisor approval before any access occurs, quarterly audits, and annual public reporting. By making improperly obtained evidence inadmissible and closing gaps that would allow informal data-selling or out-of-state sharing, SB 26-070 ensures that the warrant requirement cannot be circumvented through workarounds.

Conclusion

The Fourth Amendment does not contain a technology exception. The opposition may ask for convenience, but we are here to ask for constitutional fidelity. When those two interests clash, the Bill of Rights must prevail. Senate Bill 26-070 ensures that Colorado law keeps pace with technology while honoring the values that protect every person in this state.

I respectfully urge the Committee to advance this bill. Thank you.

Subject: Public Comment on Colorado Senate Bill 26-070
Name: Kyle Conley
Affiliation: Independent Policy Researcher; Emerging Technologies Subject Matter Expert
Date: 23 February 2026

I. Introduction

I appreciate the opportunity to submit public comment on Colorado Senate Bill 26-070. My name is Kyle Conley, and I am a Virginia-based cybersecurity and governance professional with 15+ years of experience working at the intersection of technology, law, and risk management. Throughout my career, I have worked in various capacities supporting federal law enforcement and national security functions as a senior federal employee, where I observed firsthand the operational value of data as well as the importance of clear legal guardrails governing its access and use.

In addition to my professional experience, I conduct independent research and writing focused on privacy, AI governance, and responsible data stewardship. I am currently pursuing a Doctor of Law and Policy to further examine how emerging technologies and surveillance capabilities intersect with constitutional principles and democratic oversight.

My perspective is informed not only by a commitment to civil liberties, but also by practical experience understanding how law enforcement agencies rely on structured, lawful, and defensible investigative authorities. It is from that balanced standpoint that I offer the following comments in support of SB26-070.

II. Summary of Position

I support the core intent of SB 26-070 to protect individual privacy and constrain unregulated government access to sensitive location data.[1] Modern data ecosystems increasingly aggregate granular historical location information often captured and retained by private entities for location aware marketing (LAM) which is currently accessible without meaningful oversight or clear statutory limits.[2] This data, if accessible to government entities without appropriate safeguards, threatens foundational privacy norms and may disproportionately impact civil liberties. The Supreme Court of the United States has often recognized the importance of protecting unreasonable search under the Fourth Amendment without well-defined exceptions.[3]

My professional experience working alongside federal investigative authorities has underscored both the legitimate investigative value of historical digital records and the constitutional risks associated with unstructured (warrantless) access. Legislative clarity in this area benefits not only civil liberties, but also the long-term defensibility of lawful investigations. As such, I

---

[1] Jace C Gatewood, *Warrantless GPS Surveillance: Search and Seizure-Using the Right to Exclude to Address the Constitutionality of GPS Tracking Systems Under the Fourth Amendment*, 42 The University of Memphis Law Review 303 (2011).
[2] Jing Liu, Marko M. Skoric & Chen Li, *Disentangling the Relation among Trust, Efficacy and Privacy Management: A Moderated Mediation Analysis of Public Support for Government Surveillance during the COVID-19 Pandemic*, 43 Behavior & Information Technology 551 (2024).
[3] Anonymous, *South Dakota v. Opperman: An Analysis of How Inventory Searches Are Unreasonable under the Fourth Amendment*, 98 International Social Science Review (Online) 1 (2022).

recommend clarifying certain provisions to improve legal clarity, ensure reasonable public safety exceptions, and strengthen governance safeguards while maintaining public trust.

III. Key Comments and Recommendations

1. Affirm the necessity of warrant requirements

SB 26-070's current framework effectively recognizes that location information older than a narrow window may constitute sensitive personal data requiring heightened oversight. Establishing warrant standards for access beyond basic thresholds aligns with constitutional principles that protect against unreasonable searches and access to stale data.

The availability of commercially aggregated historical GPS databases should not allow the government to obtain, in bulk, what it could not lawfully generate itself without judicial authorization. In *United States v. Jones*, the Supreme Court recognized that prolonged GPS monitoring implicates significant Fourth Amendment concerns because aggregated location data reveals patterns of life not discernible from isolated observations.[4] Permitting warrantless access to commercially compiled historical location data risks enabling precisely the type of sustained, retrospective tracking that the Court cautioned against.

2. Governance and audit requirements

Requiring policies, regular supervisory audits, and reporting is a strong governance signal, but these must be actionable and properly enforced.

3. Exceptions for urgent public safety needs

Any privacy-protective regime must allow for lawful exceptions where imminent threats or emergencies exist. However, these must be constrained and documented.

4. Data retention and deletion practices

Proposals that require deletion beyond narrow windows help minimize risks of misuse or secondary data exploitation.

IV. Closing

In summary, SB26-070 represents an important step toward clarifying and constraining government access to sensitive historical location data in a way that protects constitutional privacy interests without unduly hampering legitimate, time-bounded law enforcement needs. With additional improvements to transparency, governance, and the articulation of exceptions, this bill could serve as a strong model for future state policies balancing privacy and public safety.

Thank you for considering these comments.

Respectfully,
Kyle Conley
Independent Policy Researcher; Emerging Technologies Subject Matter Expert

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

Senate Judiciary

02/23/2026 01:30 PM

SB26-071 Use of Surveillance Technology by Law Enforcement

Typed Text of Testimony Submitted

Name, Position, Representing	**Typed Text of Testimony**
Jeany Rush For themself	TO: SENATE JUDICIARY COMMITTEE RE: SB26-071 LAW ENFORCEMENT SURVEILLANCE TECH./PROTECT CITIZENS SPONSOR: LYNDA ZAMORA WILSON FROM: JEANY RUSH, COLORADO CONSTITUENT VOTE: YES WE NEED THIS BILL! Folks: â€œSurveillance Accountability and Freedom Ensured (SAFE) Actâ€ Accountability becomes the operative word for this technology! When you add the use of â€œAIâ€ you create additional security issues, and further protections needed from errors, abuses, and theft of data. This bill is a timely need. In a time when our every action, movement, and many private actions are monitored, without our knowledge, our permission, and often in violation of our constitutional rights, it is great to discuss accountability in these actions. We all want to cooperate with law enforcement to solve and capture crime, but we do not want to have our privacy compromised to the point we no longer have any freedoms left.

	The abuses of facial recognition are worldwide already. London and Chicago, and well, China already have made their entire environments abusive in their surveillance of its citizens. The storage, filing of the data is also a serious concern. Our law enforcement does need this for cases, court, operations, however, the abuses of surveillance are a major concern. We do not want to live in a total POLICE STATE, AND THIS WOULD BE THE NATURAL BIPRODUCT OF ABUSES! EXAMPLE: â€œThe cloud Automatic License Plate Reader (ALPR or LPR) company Flock is building a dangerous nationwide mass-surveillance infrastructure, and the problem with mass surveillance is that it always expands beyond the uses for which it is initially justified! Flockâ€™s system is undergoing insidious expansion across multiple dimensions.â€ Flock sells their cloud-connected cameras to police departments and private customers across the nation!â€ This is a main reason accountability, and penalties need to exist for abuses! Colorado has sadly become a serious Traffickingâ€™ corridor, so there are real needs for these types of technology. However, victims will need protection! We do not want to tie the hands of our earnest law enforcement departments, however, we absolutely need to protect the citizens from violations of their rights! There needs to be a balance. THIS BILL GIVES THAT ACCOUNTABILITY MUCH NEEDED. WHO GUARDS THE GUARDIANS?â€
Terri Carver Against themself	I am writing an opposition to Senate Bill 26â€“071, which is a deeply flawed approach to addressing legitimate concerns about government surveillance. SB71 goes overboard in excessive administrative burdens and broad restrictions it places on law-enforcement that undermine public safety but do not further the goal of protecting individual privacy.

	It is also concerning that this bill would authorize a court to take disciplinary action (including termination) against individual police officers, when the lawsuit is against the police department and the individual officer may have been acting in good faith in reliance on police procedures and chain of command. I have not seen this type of anti-law enforcement animus in a bill since the legislation that passed after the George Floyd incident. As a State representative, I ran several bills to address concerns about government data collection on citizens. SB 71 is a badly written bill that will do significant harm to legitimate law enforcement investigations that do not encroach on individual privacy. I urge a no vote on SB 71. Terri Carver Colorado Springs
Bennett Rutledge For themself	The fourth amendment requirement for a human to supply oath or affirmation on probable cause for a warrant to get nosy is very important to us ... especially in these times when certain sworn officers feel free to lie and even sign the warrants themselves. They even seem to be protected by Qualified Immunity for such acts of perjury forgery. This bill seems anemic, but it is a step in the right direction.

Written Testimony in Support of the SB26-070 Bill

I am an engineer living in Glenwood Springs Colorado. I am extremely concerned about data security with Automated License Plate Recognition (ALPR) cameras such as Flock cameras, and I strongly support the SB26-070 bill.

I believe that technology (such as ALPR cameras) is a powerful resource, but with great power comes great responsibility. That technology must come with laws to protect citizens from abuse of that technology and power. This is why I support the SB26-070 bill and its efforts to prohibit a government entity from sharing historical location information with third parties or government agencies outside their jurisdiction.

Many people think the issue of ALPRs is only a big city issue. As a resident of Glenwood Springs on the Western Slope of Colorado, I can tell you this is a HUGE issue in our community. Glenwood Springs has more Flock cameras than any other West Slope municipality. In fact, we have more cameras total in our city than the cities of Grand Junction, Clifton, and Fruita combined, despite our city having about one tenth the population. Glenwood's citizens are intensely concerned about the issue of ALPRs and data security.

In early January, my husband and I gave public comment before our City Council to discuss our issues with ALPR cameras. Citizens have submitted online requests for better transparency. In late January, Glenwood Springs held a State of the City meeting, an opportunity for small group interactive questions, answers, and discussion about issues relevant to the City and its citizens. The event was so well attended, we overwhelmed the venue capacity. In every breakout group, I heard citizens mention concerns about the Flock cameras. City Council held an executive session on the ALPR cameras in early February. Recently, City Council has been reevaluating our contract with Flock to restrict data sharing with other entities.

Our community's main concerns include:

1. **Data security.**

   We believe it is wrong and a breach of public trust that the City is giving away our data to companies whose security cannot be trusted. Neither our City nor our Police department owns this data. We rent it. The companies we rent from - like Flock - own this data. These companies have terrible data security records.

2. **Potential Misuse of Data**

   There are many confirmed cases of data being misused and abused, especially for stalking, and false accusations. This is a real issue. I have three close friends

and family members who had to move to avoid a stalker. Let's say I moved here to avoid a stalker, but he has any connection to any law enforcement agency; he can use the Glenwood Springs Flock cameras to figure out where I live, when I leave for work every morning, where I work, when I leave work each day. There are several cameras between my house and my office, including one across the street from my office.

Glenwood Springs police department have admitted there is "nothing they can do" to prevent a "rogue officer" from accessing this data and using it illegally. Restricting the sharing of this data would help to reduce the reach of this risk.

3. **Sharing of Data with Other Government Entities (such as ICE)**

   Our community, including myself, has expressed deep concerns about ALPR location data (including face recognition) being shared with ICE. This allows the data to be used for racial profiling, putting members of our community at risk. We know ALPR data has been shared with ICE. ACLU has identified this as violation of civil liberties.

   While our City reports it does not currently choose to share its ALPR data with ICE, this could change under future administration. Furthermore, we are concerned agreements could exist between Flock and ICE that provide a "back door" for this data sharing. This is why we need laws, such as SB26-070, that govern the sharing of historical location information with third parties or government agencies outside their jurisdiction.

I understand the opposition to SB26-070. The location data provided by ALPRs is a powerful tool that can be used by law enforcement to solve crimes, such as abductions or stolen cars. However, law enforcement agencies already have the tools they need to solve these crimes, WITHOUT unrestricted sharing of data with third parties or government agencies outside their jurisdiction. We do not believe the benefit outweighs the risks and drawbacks.

In summary, the unrestricted access of location data creates a loophole that doesn't require a warrant, and violates our Fourth Amendment Rights. The unrestricted sharing of this data is a danger to us as citizens. I strongly support the SB26-070 bill.

Sincerely,

Bailey Leppek

February 23rd, 2026

Senate Judiciary Committee
200 E Colfax Avenue
Denver, CO 80203

Testimony of Chrisanna Elser in Favor of SB26-070

Chair Weissman and Members of the Senate Judiciary Committee,

My name is Chrisanna Elser. I work in the financial industry—a sector where integrity is the only currency we have. In my world, an accusation of theft is a professional death sentence. But on September 27th, that identity was nearly dismantled not by a criminal, but by an Automatic License Plate Reader (ALPR) and an officer who treated its data as gospel. I was accused of a crime I never committed and was forced to prove myself innocent.[1] I am here to testify that this technology is being sold as a shield to protect communities, but in practice, it is a digital dragnet that turns our constitutional rights upside down.

Passing SB70 will help ensure that others will never have to go through what I endured. This bill creates many crucial guardrails to protect innocent Coloradans like me from the misuse and abuse of surveillance technology. For that reason, I urge you to support it.

When Sergeant Jamie Milliman of the Columbine Valley Police Department showed up at my door. I was informed that the department had a strong case against me for stealing a package from someone's home in Bow Mar. Why? Because an ALPR flagged my forest green Rivian entering and leaving Bow Mar. He told me, "You can't get a breath of fresh air in or out of that town without us knowing."[2] This is the fundamental danger of ALPR technology: it creates an illusion of omniscience that replaces police work with algorithmic arrogance.

He had a summons for theft ready before he even spoke to me. I was faced with the dystopian task of proving my innocence against the apparently incontrovertible evidence from the system.

As a result of this, I was subjected to two weeks of living hell.

I tried desperately to reach someone, anyone from Bow Mar or Columbine Valley who would listen. I started with the Columbine Valley police chief for a week, then moved up to town administrators, and finally the mayor of Bow Mar. I was passed around, ignored, and stonewalled for fourteen days.

---

[1] See: Prentzel, O. (28 October 2025). After police used Flock cameras to accuse a Denver woman of theft, she had to prove her own innocence. *The Colorado Sun.* https://coloradosun.com/2025/10/28/flock-camera-police-colorado-columbine-valley/.
[2] *Ibid.*

While these leaders were too busy to return my calls, the Columbine Valley Police Department was active on the Neighbors app, publicly posting my vehicle and soliciting "more evidence" from the public. They were crowd-sourcing a conviction for a crime I clearly did not commit, while the people in charge of the department refused to grant me five minutes of their time.

In the course of this investigation, what was said to the homeowner, my clients, or people in my social circles? In my industry, a whisper of "theft" can end one's career.

Thankfully, I was able to collect enough data about my whereabouts to prove I could not possibly have committed this crime. My husband and I had to spend our own money to build a digital "war chest" of GPS data and dashcam footage. When the chief of police finally looked at it, he sent a flippant email saying, "nicely done, btw" as if my exoneration was a school project and not the recovery of my life.

The most damning part is that the proof of my innocence was inside the very system they control. While the crime was occurring, my truck was parked directly in front of another Flock camera at my tailor's shop. The officer simply chose to ignore the timestamps and location data that didn't fit his narrative. He focused on an AI match of someone who looked "close enough" to the thief. If he had done his due diligence, I would have been exonerated in seconds.

This technology is extremely powerful. When misused or abused, it has the power to ruin someone's life. My story is proof.

I urge you to support SB26-070. No citizen should be forced into the impossible task of proving their innocence. The guardrails this bill puts in place will help ensure there is greater accountability in how these systems are used, how the information is maintained, and when it can be accessed. Without sensible legislation, stories like mine and others that have been in the news will continue to occur.

Don't let my nightmare become the standard for our state. Please pass SB26-070.

Respectfully,

Chrisanna Elser

Denver, Colorado

February 23 rd , 2026

Senate Judiciary Committee

200 E Colfax Avenue

Denver, CO 80203

Testimony in Favor of SB26-070

Chair Weissman and Members of the Senate Judiciary Committee,

Thank you for allowing me the opportunity to speak to you today. My name is Steve Mathias. I am here today as a resident of Thornton, representing myself and the hundreds of community members who participated in a local Town Hall in-person and online to have a serious conversation about the use of Automatic License Plate Reader (ALPR) technology. As an organizer of the event, the attendance and participation I've seen on this issue underscores the urgency not only of this conversation, but also this bill. Our state needs pragmatic commonsense legislation to address this technology, and that's precisely what SB26-070 offers.

A single image is just an image. But a series of images becomes a film. And that's what widespread data collection can create. By stitching together data points across time, it is possible to create a detailed picture of ordinary people living ordinary lives, revealing where we work, where we sleep, where we learn, where we play, where we pray. When that information sits in a searchable database, it changes how safe people are. Survivors weigh whether they can safely leave an abusive home. People going to a therapist, a clinic, or a place of worship wonder who might be watching. Participants in public meetings and discussions ask whether speaking today makes them a target tomorrow. Vulnerable communities become isolated and withdrawn, because even leaving home is a risk.

This bill doesn't prohibit the use of ALPRs. It sets clear rules for when, and how far back, government agencies can look at someone's movements, while preserving rapid access in exigent circumstances, because every second counts when lives are at risk.

When an agency wants to look further back, the bill draws the right line: accessing older, historical location information should require a judicial warrant. That isn't anti-police. It's accountability, security, and safety.

The bill also limits broad retention. Unless there's a lawful reason to keep it, historical location information can't be stored indefinitely. It also limits when and how this data can be shared, so it doesn't quietly spread beyond Colorado's rules and oversight. That matters because the more data we store, and the more accessible it is, the more attractive and vulnerable it becomes for hackers, foreign governments, and other bad actors.

This bill protects us by ensuring access is lawful, limited, and accountable, so our data is shared only with the right people for the right reasons, which allows us to feel safe reporting crimes, seeking help, practicing our faith, and participating in public life.

This is a sensible, pragmatic, and commonsense way to ensure Coloradans are protected from the abuse and misuse of this technology while ensuring law enforcement has access to valuable investigative tools. For these reasons, I urge you to support SB26-070.

Thank you,

Steve Mathias

Thornton, Colorado

contact: Andrew Brandt
policy@electmorehackers.com

Testimony supporting an "amend" position to bill SB26-070

BOULDER, CO (February 23, 2026): Thank you, members of the senate judiciary committee for taking the time to read my testimony. My name is Andrew Brandt, and I am the executive director of an organization called Elect More Hackers, the purpose of which is to advise policymakers on topics relating to technology, information- and cybersecurity, data privacy, and machine learning/AI, and to recruit and train people with a cybersecurity background to run for public office. Just this month, I organized the first Hackers on the Hill event at the Colorado legislature. Thank you to the members of the committee and sponsors of this bill whose staff welcomed our delegates for those meetings.

My background includes a 19-year career in cybercrime investigations and cybersecurity research, which includes serving in the role of director of threat research for Solera Networks, Blue Coat Systems, and Symantec, and as a principal researcher at both Sophos and Netcraft, all of which provide cybersecurity products or services to government, enterprise, and household consumers. Prior to working in the cybersecurity industry, I worked as an editor and investigative journalist for the magazine PC World, covering the cybersecurity industry as a beat, and authoring the Privacy Watch column for six years.

I'm writing today in support of the "amend" position for SB26-070, Colorado's proposed version of the PEEPS Act, based on model legislation from the Institute for Justice. This important legislation is incredibly relevant given the many abuses abetted by ALPR companies, including but not limited to Flock Safety, that have already been documented in public reporting.

From a cybersecurity perspective, Flock Safety has exhibited a poor track record of responding to and addressing legitimate reports of cybersecurity vulnerabilities that have been discovered in their products. The company not only fails to remediate these products in a timely way, but the company's executives have engaged in public and private campaigns of character assassination targeting the cybersecurity researchers who have attempted to report problems and have been met with a lack of responsiveness. In the cybersecurity industry, we have developed a set of guidelines we call responsible disclosure, which dictate a set of best practices on both the reporting party and the company receiving a report about a security vulnerability in a product or service. Flock Safety has flagrantly avoided responsiveness to legitimate concerns about the company's permissiveness of poor cybersecurity practices, such as the use of a default password and no requirement for customers to enable multifactor authentication to log into the camera devices themselves, or into their management console, which controls the cameras.

Moreover, while cybersecurity and data privacy advocates have lambasted the company for overly permissive data sharing with abusive law enforcement agencies, Flock Safety CEO Garrett Langley sent an email to customers in December which characterized the people who, legitimately, have a different opinion of the role of mass surveillance in a free society as "activist groups who want to defund the police, weaken

public safety, and normalize lawlessness." In response to press questions about this email, the company went on to reply to a reporter from 404Media that "we'd be happy to speak to you about bringing justice to victims instead of activists trying to let murderers go free."

To be fair to Flock Safety and other companies that provide ALPR products to law enforcement, there have been instances in which the company's product has resulted in the successful capture of dangerous criminals. Nobody doubts that ALPR has the capability to improve safety when used in accordance with constitutional principles, such as the requirement for a judicial warrant in order to obtain information.

But ALPR products generally - not exclusive to Flock Safety's devices - also pose a clear and present danger of turning our country into a surveillance state. Flock's policies, specifically, do currently permit any law enforcement agency customer to search the company's entire dataset of location-based vehicle tracking information, nationwide. There have been multiple, documented use of law enforcement agencies using the network to hunt for vehicles and people who have sought out things like gender-specific healthcare; of individual law enforcement officers using the system to stalk or track individuals who are not the subject of a law enforcement investigation; and of federal agencies using the system to identify and track vehicles belonging to noncitizens who have been doing nothing other than peacefully going about living their lives in the United States, then targeting them with violence.

Nobody wants criminals to be able to operate with impunity, which is why the safeguards are necessary. ALPR are incredibly powerful tools, and can be used in good faith to improved public safety or, in bad faith, to oppress memebrs of the public in incredibly powerful ways. This balance of rights versus responsibilities must be maintained in light of how powerful a tool such as ALPR can be in the wrong hands.

While I have not yet seen the amendments to SB26-070 being proposed by Senator Amabile, who is my home district's senator, it is my understanding from public reporting that these amendments would loosen the restrictions in the original draft of the bill: allowing police agencies in Colorado to store up to 30 days or allow a lookback of up to 72 hours without the use of a judicial warrant.

I would urge the committee to retain the original, more restrictive language used in the initial draft of the bill, barring police from performing searches without the use of a warrant after the first 24 hours following a data collection event. I would urge the committee to consider requiring a warrant for all searches, even within that first 24 hour period. Law enforcement agencies who wish to use ALPR data in an investigation must be able to justify to a judge their need for this data, if only to curb the abusive behavior we are already seeing happening.

I further urge the committee to retain the original language that restricts data sharing among law enforcement agencies outside of the jurisdiction in which the ALPR data has been collected, in teh absence of a judicial warrant in which the agency must declare their rationale for the search, and in which reasonable limits are placed on what can be collected and used.

Thank you.

Andrew Brandt

Gmail Search mail

Compose

Inbox
Starred
Snoozed
Sent
Drafts 4
More

Labels

2020 Research Analyst
2021 Research Analyst
2022 Research Analyst
2023 Research Analyst
2024 Research Analyst
2025 Research Analyst
Digest 515
Feedback
Public Testimony
1 Registration 5,199
2 Hearing Item ... 88
3 Hearing Cancellation
CLICS Notification
OutboundstateId
zzArchives
Webex

SB26-070

External Inbox ×

tanya regan
to me

SB26-070

Good afternoon Senate Judiciary,

My name is Tanya Regan, I represent myself and I very much appreciate the opportunity to submit my testimony in support of this A

In 2008, I was a reservist at (the Former AF Space Command, now US Space Command), learning all about our satellite systems and internet technologies and data. I really wondered what kind of dystopian world we were entering – we were already in the same one government was trying to extract.

As Senator Zamora Wilson pointed out and as we all know, information in the wrong hands can and has been used against citizens. aftermath in which the Patriot Act was rapidly developed and enacted.

To understand the PATRIOT Act, one must first understand the fear and urgency that gripped America in the fall of 2001. In the imme attacks succeeded, in part, because of a failure of intelligence. A so-called "wall" existed between foreign intelligence gathering (the the hijackers was siloed within different agencies, unable to be connected into a coherent picture.

Against this backdrop, the Bush Administration rapidly drafted a massive piece of legislation, known as the PATRIOT Act of 2001. Inte national emergency, it was signed into law by President George W. Bush on October 26¸2001 - LESS THAN 50 DAYS FROM THE DATE existed, to be completed in less than 50 days - a fact that would become a central point of criticism for years to come. The Act was p prevent future attacks.

The PATRIOT Act is not a single, simple law. It is a complex package of amendments that altered over 15 existing federal statutes. Its email, cell phones, and the internet.

Unfortunately once this kind of legislation is enacted, it is difficult if not impossible to roll back. Moderation of any kind of surveillar

Thank you,

Sincerely,

Tanya S Regan

--
Tanya S. Regan
630 527 9403

Reply Forward

February 23rd, 2026

Dear Judiciary Committee Members:

I am respectfully urging a “NO” vote on the current version of SB 26-70. While I understand the bill is well-intentioned, in its present form it will significantly hinder law enforcement’s ability to solve crimes and ultimately harm victims seeking justice.

SB 26-70 does not accurately reflect the realities of criminal investigations or the practical use of Automated License Plate Readers (ALPRs). Systems such as Flock are used by the Parker Police Department only when there is reasonable suspicion to believe that a vehicle was involved in a crime, based on legally obtained information such as victim or witness statements. ALPR data is used to narrow investigations and often develop probable cause necessary to obtain search warrants for additional evidence.

Under the current version of SB 26-70, a warrant would be required to access ALPR data more than 24 hours after the occurrence of a crime. This presents two significant legal and practical problems.

First, warrants require probable cause, not reasonable suspicion.Reasonable suspicion and probable cause represent distinct constitutional standards with different evidentiary thresholds and permissible police intrusions. Reasonable

suspicion is based on specific and articulable facts that, combined with rational inferences, create reasonable suspicion of criminal activity. Reasonable suspicion is a less strict standard than probable cause but it cannot be based on a mere hunch. Probable cause, required for arrests and search warrants, requires a "fair probability" that contraband or evidence will be found based on the totality of circumstances. Generally, reasonable suspicion transitions to probable cause when law enforcement investigations uncover substantial evidence through efforts such as corroboration of informant tips through independent police observation, surveillance detecting suspicious patterns, or linking multiple reliable sources.

Using LPRs to locate vehicles involved in crimes allows officersto establish probable cause in support of search warrants to search a vehicle or home for evidence of a crime. The issue with the “warrant” requirement of this bill is that a warrant application fails if it based on a generalized search or “fishing expedition.” In most investigations, officers have reasonable suspicion, not probable cause, that a suspect vehicle passed a specific camera. Requiring a warrant to obtain LPR data creates an impossible standard and effectively eliminates ALPRs as an investigative tool.

Second, warrants must be ripe. Courts cannot grant warrants for information that may no longer exist. Because SB 26-70 limits data retention to four days, unless law enforcement establishesthat the data is less than four days old, a warrant would not be legally ripe and could not be issued. In many cases, suspects are not identified within four days. The four-day retention requirement essentially eliminates necessary evidence in most criminal investigations. This is particularly true in

complex or violent crimes. An unintended consequence of the bill, as written, is that crimes will remain unsolved, victims will not receive justice, and cold cases will increase.

The Parker Police Department has successfully used Flock to solve cases. In a recent murder case, the suspect fled immediately after the shooting. Investigators had surrounding agencies search Flock cameras in their jurisdiction in the days following the crime for a vehicle matching a specific make, model, color, and visible damage. This allowed the suspect and vehicle used during the shooting to be located within the same week of the murder. Locating the suspect so quickly stopped the destruction of evidence the suspect had started to implement. In another case Flock was used to help assist another agency locate a wanted homicide suspect by alerting to a vehicle the suspect had been driving.

These efforts ultimately identified the suspect who alluded police for two months. If SB26-70 was effective during these investigations, the cases likely would have remained unsolved. Additionally, Flock data assisted shutting down a crime spree. What needs to be stressed and the General Assembly needs to understand, these cases generally are not solved in four days. Based on the parameters of the bill, law enforcement would have been prohibited from accessing this vital evidencepotentially resulting in murder suspects remaining at-large and the continuance of the crime spree.

Flock is also routinely used to recover stolen vehicles. While not always classified as violent crimes, stolen vehicles devastate victims who rely on vehicles for transportation. Recovering stolen vehicles as quickly as possible provides immediate and

meaningful relief to the victims. That being said, SB26-70 limits access to Flock for vehicles that are actively in the process of being stolen. Many times, stolen vehicles are not reported to police as they are being stolen.

This bill appears to address concerns of illegal surveillance; however, this concern is unfounded as vehicles traveling on public roadways, including their license plates, are observable by anyone in public view where there is no reasonable expectation of privacy. Flock is not being used as an on-going surveillance tool. As stated above, it is merely a tool law enforcement utilizes when reasonable session exists that a vehicle is related to a crime. If this bill is intended to address concerns of misuse, a more balanced solution would be requiring ALPR searches be conducted only when there is reasonable suspicion that a vehicle is connected to a crime, while allowing data retention consistent with current laws.

As currently drafted, SB 26-70 would severely restrict law enforcement's ability to investigate and solve crimes, prevent justice for victims, and create a privacy interest not recognized under current constitutional law. For these reasons, I respectfully urge this committee to vote no on SB 26-70 in its present form.

Thank you for your time and consideration.

Sincerely,

Joshua R Rivero

Mayor, Town of Parker, Colorado

Testimony in Support of Colorado State Senate Bill SB26-070
By Kendall Kultgen
Leader in Arts Education, Colorado Springs & Denver

Introduction
Good afternoon, members of the committee. My name is Kendall Kultgen, and I am a leader in arts education working with under-resourced youth in both Colorado Springs and Denver. I deeply care about the well-being and safety of youth and their families. As someone who works closely with youth every day, I am concerned about the growing misuse and lack of oversight surrounding Flock surveillance technology across our state and its implications.

I'm writing to support SB26-070. In my experience, there has been a troubling lack of transparency and community input regarding the use of Flock surveillance cameras, particularly in the City of Denver. Our mayor committed to attending a public town hall to address community questions and concerns about the program but ultimately did not show and re-signed the contract with Flock without city council input. This absence of accountability and transparency shows local governments cannot be trusted to self-regulate such a powerful surveillance technology on their own.

I believe statewide guidance and regulation through SB26-070 is critical. This bill would ensure that all Coloradans receive equal protection, transparency, and safeguards concerning the use of Flock cameras. Statewide regulation would create accountability so that municipalities are not left to decide, behind closed doors, how to manage technology capable of harm.

I don't believe that Flock technology keeps communities safer. In fact, our youth and families are at more risk of harm due to the unregulated use of evidence from this technology. The ACLU found that Flock data has already been accessed by agencies like ICE and the Department of Homeland Security, posing real dangers to immigrant and marginalized communities. Without strong regulation, this technology can and has fallen into the wrong hands. Far from making us safer, it risks enabling unjust surveillance and misuse.

For the sake of our youth and our families, I urge you to support SB26-070. We have an opportunity today to keep our communities safe through the regulation of Flock technology use.

Thank you for your time and consideration.

Kendall Kultgen

contact: Andrew Brandt
policy@electmorehackers.com

Testimony supporting an "amend" position to bill SB26-070

BOULDER, CO (February 23, 2026): Thank you, members of the senate judiciary committee for taking the time to read my testimony. My name is Andrew Brandt, and I am the executive director of an organization called Elect More Hackers, the purpose of which is to advise policymakers on topics relating to technology, information- and cybersecurity, data privacy, and machine learning/AI, and to recruit and train people with a cybersecurity background to run for public office. Just this month, I organized the first Hackers on the Hill event at the Colorado legislature. Thank you to the members of the committee and sponsors of this bill whose staff welcomed our delegates for those meetings.

My background includes a 19-year career in cybercrime investigations and cybersecurity research, which includes serving in the role of director of threat research for Solera Networks, Blue Coat Systems, and Symantec, and as a principal researcher at both Sophos and Netcraft, all of which provide cybersecurity products or services to government, enterprise, and household consumers. Prior to working in the cybersecurity industry, I worked as an editor and investigative journalist for the magazine PC World, covering the cybersecurity industry as a beat, and authoring the Privacy Watch column for six years.

I'm writing today in support of the "amend" position for SB26-070, Colorado's proposed version of the PEEPS Act, based on model legislation from the Institute for Justice. This important legislation is incredibly relevant given the many abuses abetted by ALPR companies, including but not limited to Flock Safety, that have already been documented in public reporting.

From a cybersecurity perspective, Flock Safety has exhibited a poor track record of responding to and addressing legitimate reports of cybersecurity vulnerabilities that have been discovered in their products. The company not only fails to remediate these products in a timely way, but the company's executives have engaged in public and private campaigns of character assassination targeting the cybersecurity researchers who have attempted to report problems and have been met with a lack of responsiveness. In the cybersecurity industry, we have developed a set of guidelines we call responsible disclosure, which dictate a set of best practices on both the reporting party and the company receiving a report about a security vulnerability in a product or service. Flock Safety has flagrantly avoided responsiveness to legitimate concerns about the company's permissiveness of poor cybersecurity practices, such as the use of a default password and no requirement for customers to enable multifactor authentication to log into the camera devices themselves, or into their management console, which controls the cameras.

Moreover, while cybersecurity and data privacy advocates have lambasted the company for overly permissive data sharing with abusive law enforcement agencies, Flock Safety CEO Garrett Langley sent an email to customers in December which characterized the people who, legitimately, have a different opinion of the role of mass surveillance in a free society as "activist groups who want to defund the police, weaken

public safety, and normalize lawlessness." In response to press questions about this email, the company went on to reply to a reporter from 404Media that "we'd be happy to speak to you about bringing justice to victims instead of activists trying to let murderers go free."

To be fair to Flock Safety and other companies that provide ALPR products to law enforcement, there have been instances in which the company's product has resulted in the successful capture of dangerous criminals. Nobody doubts that ALPR has the capability to improve safety when used in accordance with constitutional principles, such as the requirement for a judicial warrant in order to obtain information.

But ALPR products generally - not exclusive to Flock Safety's devices - also pose a clear and present danger of turning our country into a surveillance state. Flock's policies, specifically, do currently permit any law enforcement agency customer to search the company's entire dataset of location-based vehicle tracking information, nationwide. There have been multiple, documented use of law enforcement agencies using the network to hunt for vehicles and people who have sought out things like gender-specific healthcare; of individual law enforcement officers using the system to stalk or track individuals who are not the subject of a law enforcement investigation; and of federal agencies using the system to identify and track vehicles belonging to noncitizens who have been doing nothing other than peacefully going about living their lives in the United States, then targeting them with violence.

Nobody wants criminals to be able to operate with impunity, which is why the safeguards are necessary. ALPR are incredibly powerful tools, and can be used in good faith to improved public safety or, in bad faith, to oppress memebrs of the public in incredibly powerful ways. This balance of rights versus responsibilities must be maintained in light of how powerful a tool such as ALPR can be in the wrong hands.

While I have not yet seen the amendments to SB26-070 being proposed by Senator Amabile, who is my home district's senator, it is my understanding from public reporting that these amendments would loosen the restrictions in the original draft of the bill: allowing police agencies in Colorado to store up to 30 days or allow a lookback of up to 72 hours without the use of a judicial warrant.

I would urge the committee to retain the original, more restrictive language used in the initial draft of the bill, barring police from performing searches without the use of a warrant after the first 24 hours following a data collection event. I would urge the committee to consider requiring a warrant for all searches, even within that first 24 hour period. Law enforcement agencies who wish to use ALPR data in an investigation must be able to justify to a judge their need for this data, if only to curb the abusive behavior we are already seeing happening.

I further urge the committee to retain the original language that restricts data sharing among law enforcement agencies outside of the jurisdiction in which the ALPR data has been collected, in teh absence of a judicial warrant in which the agency must declare their rationale for the search, and in which reasonable limits are placed on what can be collected and used.

Thank you.

Andrew Brandt

Written Testimony in Support of the SB26-070 Bill

I am an engineer living in Glenwood Springs Colorado. I am extremely concerned about data security with Automated License Plate Recognition (ALPR) cameras such as Flock cameras, and I strongly support the SB26-070 bill.

I believe that technology (such as ALPR cameras) is a powerful resource, but with great power comes great responsibility. That technology must come with laws to protect citizens from abuse of that technology and power. This is why I support the SB26-070 bill and its efforts to prohibit a government entity from sharing historical location information with third parties or government agencies outside their jurisdiction.

Many people think the issue of ALPRs is only a big city issue. As a resident of Glenwood Springs on the Western Slope of Colorado, I can tell you this is a HUGE issue in our community. Glenwood Springs has more Flock cameras than any other West Slope municipality. In fact, we have more cameras total in our city than the cities of Grand Junction, Clifton, and Fruita combined, despite our city having about one tenth the population. Glenwood's citizens are intensely concerned about the issue of ALPRs and data security.

In early January, my husband and I gave public comment before our City Council to discuss our issues with ALPR cameras. Citizens have submitted online requests for better transparency. In late January, Glenwood Springs held a State of the City meeting, an opportunity for small group interactive questions, answers, and discussion about issues relevant to the City and its citizens. The event was so well attended, we overwhelmed the venue capacity. In every breakout group, I heard citizens mention concerns about the Flock cameras. City Council held an executive session on the ALPR cameras in early February. Recently, City Council has been reevaluating our contract with Flock to restrict data sharing with other entities.

Our community's main concerns include:

1. **Data security.**

   We believe it is wrong and a breach of public trust that the City is giving away our data to companies whose security cannot be trusted. Neither our City nor our Police department owns this data. We rent it. The companies we rent from - like Flock - own this data. These companies have terrible data security records.

2. **Potential Misuse of Data**

   There are many confirmed cases of data being misused and abused, especially for stalking, and false accusations. This is a real issue. I have three close friends

and family members who had to move to avoid a stalker. Let's say I moved here to avoid a stalker, but he has any connection to any law enforcement agency; he can use the Glenwood Springs Flock cameras to figure out where I live, when I leave for work every morning, where I work, when I leave work each day. There are several cameras between my house and my office, including one across the street from my office.

Glenwood Springs police department have admitted there is "nothing they can do" to prevent a "rogue officer" from accessing this data and using it illegally. Restricting the sharing of this data would help to reduce the reach of this risk.

3. **Sharing of Data with Other Government Entities (such as ICE)**

   Our community, including myself, has expressed deep concerns about ALPR location data (including face recognition) being shared with ICE. This allows the data to be used for racial profiling, putting members of our community at risk. We know ALPR data has been shared with ICE. ACLU has identified this as violation of civil liberties.

   While our City reports it does not currently choose to share its ALPR data with ICE, this could change under future administration. Furthermore, we are concerned agreements could exist between Flock and ICE that provide a "back door" for this data sharing. This is why we need laws, such as SB26-070, that govern the sharing of historical location information with third parties or government agencies outside their jurisdiction.

I understand the opposition to SB26-070. The location data provided by ALPRs is a powerful tool that can be used by law enforcement to solve crimes, such as abductions or stolen cars. However, law enforcement agencies already have the tools they need to solve these crimes, WITHOUT unrestricted sharing of data with third parties or government agencies outside their jurisdiction. We do not believe the benefit outweighs the risks and drawbacks.

In summary, the unrestricted access of location data creates a loophole that doesn't require a warrant, and violates our Fourth Amendment Rights. The unrestricted sharing of this data is a danger to us as citizens. I strongly support the SB26-070 bill.

Sincerely,

Bailey Leppek