

**HOUSE OF REPRESENTATIVES
COMPILATION OF PUBLIC COMMENTS**

Submitted to the Committee on Delivery of Government Efficiency

For Hearing Date: Wednesday, August 19, 2026 9:00 AM

Compiled on: August 19, 2026 5:10 PM

Note: Comments received by the committee reflect only the view of the individual(s) submitting the comment, who retain sole responsibility for the content of the comment. Neither the committee nor the Texas House of Representatives takes a position on the views expressed in any comment. The committee compiles the comments received for informational purposes only and does not exercise any editorial control over comments.

COMMENTS FOR Data Privacy and Security

Zachary Burkhalter

Self/cook

Amarillo, TX

Mass surveillance should not even be considered when the only excuse is criminal activity, even when all law enforcement will do is listen & comply whole heartedly listen to an AI infrastructure, and believe whatever this entity says. Even now, it's being abused to stalk people for their own personal gain, legal or not, then the punishments are not severe enough for those who are the actual criminals in our own law enforcement, house seats, etc. All flock cameras is in infringement on ordinary citizens rights and should all be cut from all tax payer dollars. We are fast tracked to losing all right to move freely without something/somebody tracking your every move in hopes that ordinary citizens are just expected to slip up. BAN ALL TRACKING CAMERAS.

William Gonzalez

Self

Leander, TX

As a vet I served this great country upholding our constitution from enemies foreign and domestic. These flock cameras and others like them are against our constitution we deserve the right to travel in peace. When we get to our destination and go inside a private building its a different story. But for our government to watch us and catalog our every movement... seems like a domestic enemy.

JOSE PENA

Self citizen

WESLACO, TX

Dragnet surveillance is not needed as it makes it so that anyone wether or they are or aren't determined to be guilty it also creates a 4th amendment violation since if warrants are needed for cell phone locations you would also need the same for ALPR'S and other surveillance state products such as axon etc.

Seth Lipko

Self

Waller, TX

Regarding ALPRs and other technologies used for mass surveillance, there MUST be guardrails placed on these new tools. We cannot just blindly walk into this new era of tech, AI-enabled pattern building, and massive connected networks of tracking systems. I support the complete removal of ALPRs, but understand that the legal implications are steep to accomplish such as task, and also acknowledge that these tools are beneficial to law enforcement to catch actual criminals.

This is not a reason to violate upstanding citizen's rights.

So in a good faith effort to meet in the middle, I believe that MINIMALLY, two safeguards should be enforced:

- end public funding (aka grant money) for these systems, so that MY tax dollars aren't used to unconstitutionally invade my privacy
- enforce flock and other contractors to adhere to the Texas Data Privacy and Security Act, to better protect my information that is being collected against my will, without my consent.

Additionally, I think there should be limitations and restrictions on the locations of these devices. Within 2 miles of my home, there are several cameras that are owned by up to 4 DIFFERENT jurisdictions (HOA, city, county, and state). Not only is that wasteful, if each agency can request the records from another, it's also a ridiculous overuse, and reasonably meets suspicion of MASS surveillance. Each individual jurisdiction says "oh we only have X cameras" knowing full well they can request records from the totality of the cameras in the network. There is no upper bound, and that is a huge miss that should be addressed. Some ideas: Per capita limits on quantities, restrict installations to major roadway intersections only, no invasive private property visibility from the camera point of view, etc.

Thank you for considering and acting to protect my privacy rights!

Caleb Lipko

Self

Bryan, TX

End all taxpayer subsidies and government funding for municipal ALPR programs. We don't want to live in a surveillance state. Force all ALPR companies to comply with the Texas data privacy and security act. No more indefinite tracking, cross agency sharing, and commercial data gathering. Protect the 4th amendment!

Ivan Svrcek

Self, professional engineer

Bryan, TX

Warrantless mass surveillance in the form of ALPR camera networks is running rampant in Texas and needs to be stopped. They are a form of drag-net surveillance conducted against every innocent citizen with no meaningful guardrails in place. They are a huge privacy vulnerability that is being imposed upon everyone with no choice.

We need action:

#1- Remove the funding source: MVCPA is fueling this network with grants. The MVCPA was not made for citizens, it was made by/for insurance companies and they should not be funding an invasion of citizens privacy. Prohibit usage of MVCPA funds for mass surveillance.

#2-Charge large private business which are participating in wide scale surveillance and sharing ALPR data with stalking. Large retailers are sharing data with each other to track citizens and also sharing with the government to increase the scope and create more perfect surveillance. This is stalking by a private entity and should be treated as such.

#3-Enforce public visibility and oversight of all systems. Local law enforcement have been blocking public information requests to see search audits, operational capabilities and other information. The AG office has in many cases been backing up these withholdings despite Texas law on the matter. Accessing this information is a right of the people and there can be no justifiable reason to prevent the citizens from seeing what their government is doing.

#4- Force all companies that engage in this behavior to be publicly accountable. Make a law requiring any company that shares ALPR / surveillance data in a network larger than the confines of their single geographic store be accountable to public records requests so they must divulge their activities and search histories. They are acting in a capacity of law enforcement and must be accountable as such.

#5-Require auditable records for the transmittal of all ALPR/ video/ photographic/ or other tracking metadata. Make a law requiring an audit trail that logs every time an image or metadata is transmitted from a collection site to a server and then downloaded or accessed from that server. Existing systems only support some information about searches but no custody of records themselves.

#6- Require warrants to collect data. These systems are a play to get around warrant requirements for cellphone data. Every important reason to implement a system like this should be readily supported by a warrant. Missing children, stolen cars, any other crime is already something that a warrant can be obtained for.

#7- Prohibit location history. ALPR system sensors should operate as a hotlist lookup only. Upload a new plate to the network and allow each device to look for a plate that is on the list. Do not transmit any information back to a historical database unless it is a hit on a hotlist plate that has been added to the system with a valid warrant.

Kody Fox
Self
College Station, TX

Flock, Axon and other ALPR cameras that have the ability to link nation wide citizen data to a singular, searchable database is like hiding all of our nuclear launch codes in one file on a server. There are no promises that this company won't make back door deals. There are always vulnerabilities in any system, which flocks specific vulnerabilities can be found, filed on the National Vulnerabilities Database. This data base is managed by DHS. A singular company should not be able to host this amount of data on their own private servers. They say the customer owns the data, but the license granted to them gives them all the rights to do anything they want with the data. Ultimately, the vast majority of the people do not want to drive around knowing big brother is watching. If the people don't want it, it should not be installed. Plain and simple. We are a democratic republic, and at the state level we elect officials to make decisions that will benefit our community, and set us up for success in the future. This system will inevitably be used against us. Whether a foreign adversary, or domestic tyrant, it will systematically be used against the citizens of the United States of America, should it continue to wedge its way into our infrastructure. The people who advocated, and allowed this to happen will be remembered as cowards. Please ban ALPRs and mass surveillance systems in Texas. Draw the line. Take the stand. And do what is right.

Mercy Hunter
SELF
ELGIN, TX

this must end! Flock cameras raise serious Fourth Amendment concerns by allowing government agencies to collect, store, search, and share citizens' location data without individualized suspicion or a warrant. This mass surveillance creates substantial potential for abuse, unauthorized tracking, government overreach, and violations of privacy and constitutional rights.

Lesha Roberts
self
Hockley, TX

CLOSE THE TDPSA VENDOR LOOPHOLE & END PUBLIC SUBSIDIES. For every case of a crime being solved, there are examples of innocent people being wrongly accused due to misread license plates, system errors, or law enforcement misuse. Additionally, almost daily now you hear about law enforcement personnel fired for using the FC System inappropriately including for harassment, stalking, and retaliation. FC technology goes beyond standard license plate readers; it can identify vehicles by specific details such as dents, markings, and customizations. And, control over the release of this data belongs entirely to the subscription holder, not the individuals being surveilled. According to Business Insider, FS monitors it's misread rates, but does not release this data publicly. Performance varies based on license plate design, lighting, and typeface. Because rules vary by state and lack federal standards, license plates have a wide range of clarity, creating a wide margin for error. A study by the Electronic Frontier Foundation found that only 0.5% of license plate scans were connected to a hotlist, meaning 99.5% of captured plates belonged to innocent citizens. Marc Andreessen is FC's largest institutional investor, has a long laundry list of privacy violations involving the monetization of personal data. (Cambridge Analytica scandal 87M FB users). In response to broader surveillance concerns, U.S. Congressman Tim Burchett introduced a bill to prevent federal agencies from purchasing or accessing automated surveillance systems.

Marilyn Lang
SELF/SMALL BUSINESS OWNER
sealy, TX

Close the TDPSA vendor loophole and end subsidies for ALPR surveillance.

John Hocutt, PMP
Aelf
Cypress, TX

I Demand lawmakers close the TDPSA vendor loophole & end public subsidies for ALPR surveillance!

Steve Greiner, Dr. COL (Retired). US Army
self
Cuero, TX

Please take actions to eliminate Flock surveillance cameras and the intrusion on citizens' reasonable expectation of privacy. Loss of freedom doesn't happen all at once. First it starts with cameras on every road - "for safety", then stores stop taking cash - "for convenience", then comes digital ID - "for efficiency". Each step arrives and is put in place for a nice reason and not a single one was ever on a ballot. Nobody asked - nobody ever asks they just do it. That is how you boil a frog.

Jeramy Kitchen
Texas Policy Research Action
Weatherford, TX

Thank you for the opportunity to provide comments regarding implementation of the Texas Data Privacy and Security Act (TDPSA). The TDPSA established a strong statewide framework by giving Texans greater ability to access, correct, delete, & obtain copies of their personal data, opt out of certain processing activities, & expect greater transparency & reasonable security practices from businesses. Future reforms should build on that framework without creating unnecessary barriers to innovation and free enterprise. One area deserves greater attention: government itself. The TDPSA largely exempts state agencies & political subdivisions, even though Texans routinely provide government with sensitive information through driver's licenses, tax & property records, court filings, professional licenses, & other interactions. Government should meet the same high standards of stewardship it expects from the private sector. The Supreme Court's recent *Chatrre* decision reinforces this concern. The Court held that obtaining historical location information through a geofence warrant constitutes a Fourth Amendment search. Constitutional privacy protections should not disappear simply because technology makes large-scale collection possible. Rather than regulating each new surveillance technology separately, Texas should establish durable standards governing government collection, retention, & use of personal information. Warrants supported by probable cause should remain the default for obtaining detailed location information, subject to narrowly defined emergency exceptions. Surveillance should be particularized & based on individualized suspicion rather than broad collection designed to identify suspects afterward. Agencies should minimize data collection, limit retention of information concerning people never suspected of wrongdoing, & provide meaningful transparency through public reporting and independent audits. The Legislature has already encountered these concerns. During the 89th Legislature, House Bill 961 by Representative Harrison & House Bill 2083 by Representative Bucy III proposed different safeguards for automated license plate reader data. Neither received a committee hearing. The bipartisan interest demonstrates that government surveillance & data privacy are not inherently partisan concerns. Lawmakers should also proceed cautiously before imposing additional mandates on private companies. Requirements such as broad age verification or online monitoring can force platforms to collect even more sensitive information, potentially undermining the privacy they seek to protect. Parents, rather than government, should remain the primary decision-makers regarding their children's online activity. Our Texas Liberty Compact calls for protecting free speech & digital expression, limiting government, & preserving individual liberty.

Travis Cramer-Orozco
Self/welder
Georgetown, TX

Who gave you the right to ignore the 4th amendment?

Matthew Respondek
self, teacher
Mansfield, TX

Data privacy is a major concern for myself and many Texans. Companies do not have a right to our data but they act like they do. Companies should ask consent to collect data and clearly inform users that their data is being collected, as well as why it is being collected. We need clear and common sense guidelines on data privacy that put users first. We need to make privacy the expectation, not the goal and the AG office should be at the forefront of this fight.

Nathaniel Boutin
Self
Carthage, TX

I am opposed of having my privacy breached when I have not committed any crimes. I will vote against anyone supporting the use of audio and video recording devices that can track or put together a picture of where i go and when
This is a violation of our 4th amendment rights even though the Supreme Court hasn't ruled on it. We the people under the constitution still have the power to to push back against this tyranny.

Kevin Thomas
Self
Hockley, TX

Texas banned automated red-light ticketing cameras statewide in June 2019 via House Bill 1631. This is much worse and further oversteps our right to privacy. This is a third party that is collecting our information and we have no access. We also don't know who all has access and what they can do with it, but it's at our cost? Why are we paying for a warrantless search of all citizens? We have already seen numerous counts of individuals misusing this technology on the back of a law that removed red-light cameras, why are we now allowing a more invasive system that's ran by an independent company with little to no restrictions?

Mary Ellen Cuzela
Self
Katy, TX

4th Amendment rights must be protected; stop warrantless location dragnet searches; hold contractors to same strict privacy standards; taxpayers should never be funding these 4th Amendment violations; reign in Big Tech tracking

Brandy Hughes
Self
Wortham, TX

I urge you to oppose the use of flock cameras. While public safety is important, widespread license plate, surveillance raises, serious concerns about privacy, data retention, and potential tracking of innocent people. Texans deserve effective law enforcement without unnecessary, continuous monitoring of their movements.

Bruce Cramer
self
San Antonio, TX

ALPRs present a problem in that my right to privacy is not safe with them.

Josh Posey

Self

Waller, TX

Members of the Committee, I am submitting this comment to ask you to close the loophole in the Texas Data Privacy and Security Act that lets private camera companies track innocent drivers across our state. On my way to attend this hearing today, I drove past 11 automated license plate cameras. Every single one logged my location, direction, and travel time simply because I chose to exercise my right to participate in our government. This is not targeted law enforcement. It is mass surveillance of everyday people going about their daily lives.

What makes this worse is that Texas taxpayers are financing the very systems used to monitor them. Private companies build these camera networks using taxpayer dollars and government subsidies, turning a profit at the expense of our privacy. We should not have to foot the bill for our own surveillance. The Legislature must strictly limit and eliminate state funding and subsidies for private license plate reader networks. Public funds should never be used to finance corporate tracking systems that log the movements of innocent citizens.

When private companies collect and hold this location data, it threatens our basic constitutional rights. Whether someone is driving to a doctor, a political rally, a house of worship, or a legislative hearing, their movements are recorded without a warrant. Storing this information in private databases creates serious security risks, including data breaches and unauthorized access. It also lets government agencies bypass Fourth Amendment warrant requirements by purchasing or requesting location records directly from private vendors.

To protect Texans, the Legislature needs to update our state privacy laws. We must remove commercial exemptions for private camera companies, stop providing state subsidies for surveillance networks, and require law enforcement to obtain a search warrant based on probable cause before accessing location databases. Furthermore, any camera scan that does not match an active criminal alert should be deleted immediately. States like New Hampshire already lead the way by requiring non matching scan data to be purged within 3 minutes. Texans should not have to pay for the infrastructure that tracks them on public roads. Please close the exemption loophole and protect our freedom.

Daniel Woislav, ESQ.
Institute for Justice
Austin, TX

Chairman Capriglione, Vice Chair Bhojani, and Members of the Committee,

My name is Daniel Woislav, an attorney at the Institute for Justice (IJ), a national nonprofit dedicated to ending abuses of government power and securing constitutional rights. Through our Project on the Fourth Amendment, we have challenged the largely unregulated use of Automatic License Plate Readers (ALPRs). We urge the Committee to recommend statutory ALPR guardrails in 2027. Taxpayer funded surveillance contracts operating under no statewide standard for warrants, retention, or interagency sharing are exactly the unaccountable government spending this Committee was created to examine.

ALPRs photograph every passing vehicle and use artificial intelligence to read license plates and detect other vehicle features, allowing police to identify a driver and see where they have traveled. This data feeds into a centralized, searchable database accessed with little oversight, revealing intimate details about law abiding motorists' lives.

Flock Safety alone contracts with more than 5,000 agencies nationwide, with nearly 100,000 cameras across more than 6,000 communities. Texas is one of its largest markets, with an estimated 10,000-plus cameras statewide. DPS has spent \$26 million on its own Flock contract for Operation Lone Star, and its data sharing partnerships grew from 122 agencies in February 2026 to 206 by early August, a 69 percent increase in five months.

Recent headlines detail abuse: Baytown, Pasadena, and Fort Bend County officers faced investigations or resigned over misuse of Flock systems to track colleagues or family members. Flock itself operated in Texas without the required security license from 2019 to 2024, prompting a DPS cease and desist letter and a fine.

Texas has no statewide law governing ALPR access, retention, or sharing. IJ's model legislation, the PEEPS Act, would fill that gap: a warrant requirement to access historic location data (excluding exigencies), a prohibition on sharing data outside the collecting jurisdiction without a warrant, and formal audit procedures. Similar legislation, HB 961 of the 89th Legislature, did not advance last session; we urge the Committee to help build the record needed to revisit this in 2027.

Warrants provide critical judicial oversight, and probable cause is not a high bar when officers have an actual reason to access data. Exigent circumstances remain exempt. Retention limits matter because any database risks compromise; Harris County alone just renewed its 480 camera contract for roughly \$869,000. Sharing restrictions keep Texans' data subject to Texas law, and audits ensure compliance.

Together, these guardrails create a floor of responsibility, and Texas has an opportunity to lead the nation.

We urge the Committee to recommend ALPR legislation modeled on the PEEPS Act.

Respectfully,
Daniel Woislav
Attorney, Institute for Justice
dwoislav@ij.org

Lisa Horton
self
Humble, TX

to our "leaders", the surveillance is backwards. we should be watching you! stop the collection of our data without our consent!

Patricia Brooks, Mrs
Myself
New Braunfels, TX

End ALPR, drones and any law agency from using mass surveillance against its citizens without a warrant.

Michael Frazier, Dr.
Self
Silsbee, TX

As a concerned Texas citizen, I ask the Texas Legislature to establish meaningful statutory safeguards governing the use of Automated License Plate Reader (ALPR) systems, including those operated through the Flock Safety network.

I recognize that ALPR technology can be a valuable investigative tool. When used appropriately, it can help recover stolen vehicles, locate missing persons, and assist law enforcement in solving serious crimes. My concern is not with lawful, targeted use of this technology, but with the absence of clear limits on its collection, retention, sharing, and warrantless use.

Every passing vehicle is capable of being recorded, timestamped, and geolocated, creating a detailed historical record of the movements of ordinary Texans who are not suspected of any crime. When this information is retained for extended periods and shared across a large network of agencies, it enables a level of mass location tracking that was never contemplated when our constitutional protections against unreasonable searches were established.

Texas should not permit unrestricted access to historical location data without meaningful judicial oversight. If law enforcement seeks to reconstruct a person's movements over time through historical ALPR data, that access should generally require a warrant supported by probable cause, except (perhaps) in clearly defined emergency circumstances. Similar guardrails already exist for other forms of sensitive digital information.

I also urge the Legislature to require:

- * Transparent policies governing ALPR deployment and acceptable use.
- * Strict data retention limits, ensuring data is not stored longer than necessary, such as a maximum of 30 days.
- * Detailed audit logs documenting every search and query, and public access to searches conducted where their data is included.
- * Criminal penalties for intentional misuse or unauthorized access.
- * Annual public reporting on system usage, data sharing, and compliance.
- * Independent oversight and periodic audits to ensure accountability.

Technology should enhance public safety without eroding the privacy rights of law-abiding citizens. Strong oversight protects both the public and law enforcement by ensuring these powerful investigative tools are used appropriately and consistently.

Texas has long been a leader in defending individual liberty and constitutional rights. I respectfully ask you to enact legislation that preserves the legitimate benefits of ALPR technology while establishing reasonable safeguards against warrantless surveillance, mission creep, and abuse. Public safety and personal privacy are not competing values—they are both essential to a free society.

Benjamin Bonney

Myself

Childress, TX

All mass surveillance cameras like flock cameras and the new DSP vehicles just purchased for mass surveillance which breaks our constitution 4th amendment protecting our privacy need to be removed from everywhere in the state of Texas ASAP!

For myself speaking in November I will be voting out everyone in office that's allowed these things in Texas! And the Ai data mass surveillance centers.

This is America the land of the free and a constitution that limits the government, we aren't China!!!

I can't believe our state leaders and representatives do this to Texans..

A citizens data belongs to the citizen not any private businesses and not the state of Texas and or the federal government! I expect you people in Texas government to protect us citizens!

If you all in office now can't or won't I will be voting and getting other Texans to vote y'all out for folks who will follow the constitution that each one of you took a oath to follow.
