

MONICA ALPONTE — Libertarian Candidate, House of Representatives, Arizona Dist 1

FLOCK CAMERAS — I OPPOSE!

aka "Interconnected AI-Powered Mass Surveillance Networks;" Flock Safety (Flock Group Inc.), Motorola Solutions (Vigilant), Axon, Verkada, and other equivalent systems.

***THE FOURTH AMENDMENT TO THE U.S. CONSTITUTION**:*

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Per the 2026 Senate Judiciary Committee Subcommittee on Crime and Counterterrorism Hearing Record: [1]

FACT: 👉 **"Flock cameras" Flock Safety (Flock Group Inc.) is only one brand of interconnected, AI-powered, networked surveillance cameras. There are others, like Motorola Solutions (Vigilant)**, **Axon**, **Verkada**, and other equivalent systems that link multiple cameras across locations using AI to search stored records and allow people's movements to be tracked over time. [1]

FACT: 👉 **Access is not limited to law enforcement**. Customers like **homeowners' associations**, **apartment managers**, **businesses**, **schools**, **private communities**, and **individuals** can purchase such camera systems. Any private citizen with a credit card and a subscription may be able to buy into these tracking networks, and depending on the system and access permissions, they may also be able to search camera footage, access cross-state data, or grant law enforcement direct access to their feeds. At this time there is **no federal statutory framework or prohibition** stopping these companies from selling to private buyers. [1]

FACT: 👉 At this time, **no warrant is required** to build or access Flock cameras or interconnected, AI-powered, networked surveillance cameras. There are no mandatory corporate or government cybersecurity safeguards or oversight, and these integrated platforms are completely vulnerable to hacking. [1]

WHY I OPPOSE FLOCK CAMERAS (aka Interconnected AI-Powered Mass Surveillance Networks)

• Just because we CAN spy DOESN'T mean WE SHOULD.
• We simply **do not need that much data**. We don't need AI tracking citizens on public streets any more than we need cameras monitoring our public restrooms or our neighbors' homes.
• **AI policing** our streets, public sidewalks to identify people, analyze behavior, and monitor public spaces like in communist China or North Korea is Orwellian, un-American, and incompatible with a free and democratic society.
• Our **current traditional traffic cameras (non-AI)** are sufficient. **Point-in-time automated license plate readers (ALPRs)** already act as digital eyes for localized, common-sense policing—identifying stolen vehicles and matching active **AMBER Alerts** without tracking law-abiding citizens. [1]
• **Flock cameras enable warrantless tracking** of people's present and past movements across locations. These systems are fallible, vulnerable to abuse, and unconstitutional under the Fourth Amendment and privacy laws.
• **There have already been at least 27 documented cases** of life-altering mistakes involving license plate reader systems that led to innocent people being wrongly stopped, arrested, or jailed, like **Lindsay Isaacs** [1] **who was falsely charged with vehicular homicide facing life in prison!** (Of the 27 cases: 21 involved FLOCK CAMERAS; 1 involved Rekor; 1 involved NDI, and 4 did not identify the camera brand.) **As far as I'm concerned even 1 is too many!**

Senate Judiciary Committee Subcommittee Hearing on Crime and Counterterrorism (Hearing held September 23, 2026)
Source Material: Youtube https://youtu.be/KCEdX3o5KfU?si=lYnpXMMrvPsCtDZr&t=1
"Senator Hawley EXPOSES The Network of FLOCK CAMERAS Across The Country"



Senator Josh Hawley

==========

[1] Senate Judiciary Committee Subcommittee Hearing Transcript:

CHAPTER 1: OPENING REMARKS

Chairman Hawley: Well, let me call to order this **hearing of the Senate Judiciary Committee Subcommittee on Crime and Counterterrorism**, which I'm delighted to chair and to work on with my colleague, **Ranking Member Durbin**. Thank you to all of our witnesses for being here. Welcome to all of our guests who are here today in the gallery. This hearing is about a simple thing. It's trying to get to the bottom of what is going on with the expanding surveillance network that appears to be going coast to coast in this country. I have in mind the hundreds of thousands of individual cameras, all linked to the cloud, all powered by AI that seem to be spreading all across the country. Practically every state in the union now has them. **Hundreds of thousands of them, recording billions of images every single month.**

And the question is, where are all of these images going? Who's using them? What are the privacy protections for them? How do we make sure that this kind of surveillance is consent with the Constitution of the United States? You know, there's many players in this industry. But there's one name that really stands out above the rest, and that is **Flock**. If you haven't heard of **Flock**, all I have to say is **Flock's** probably heard of you. In fact, the truth is you have probably been scanned and surveiled and tagged and logged multiple times this week alone. And that's because **Flock**, by its own admission and its own statistics, **maintains a network of 120,000 individual cameras in 49 states all across this country. It estimates that those cameras scan and then generate some 20 billion images—that's with a B—20 billion images every single month.**

Flock is a privately held company based on what we know. It's backed by a venture capital firm. It's worth about $10 billion and it has amassed in a very short time frame a surveillance network unlike any we've ever seen in this country. And really what makes it unique based on what we can tell from the reporting and the reporting on what these networks can do, I have to tell you, is really kind of wild. What seems to make these networks unique is not just the sheer number of cameras, is the fact that they're all linked together and powered and searchable by AI. It's unlike anything we've ever seen in this country before.

And to give you just a sense of it, I mean, here is some of what these cameras can do. This surveillance network uses thousands of these AI powered cameras to capture and analyze images of passing vehicles. Let's see if we can give you a sense of it. Here's a **Flock** image. **They store and catalog details like the vehicle's make, model, color, location, date, time. Flock's searchable features include details like dents and roof cracks and vehicle damage and racks on the roof or racks on the back or specific bumper stickers even.** You think about that. I mean, **Flock** can tell you if a car has a Trump sticker or a Harris sticker or a Pro-life America sticker or an NRA sticker. It's really quite extraordinary.

Flock's cameras can even recognize whether people are in the images. And in fact, in fact, **Flock admitted in a letter to me ahead of this hearing that you could search their database based on people's images. You could ask to search people, images that had people, images that are scanning the inside of the cars.** I mean this is really quite extraordinary. **Flock** is not the only player in this field. Of course there are other companies **Motorola**, **Axon**, **Vercada**, and they've also built these vast surveillance networks that are also supercharged by AI. And the thing is when you harness all of these things together, you get a capability based on the reporting that is different in kind than anything we've ever seen in this country.

And I just want to state right now my principal concern with all of this. Number one, I just want to get the facts as to what these networks are, how they operate, what they're doing. But I also just want to say this, and I want to be clear about it. The Constitution of the United States is just as valuable and valid and applicable today as it was almost 250 years ago when it was first pinned. And that includes the right to be innocent until proven guilty. That is not treated like a criminal and tracked like one. It includes the right to personal privacy, control of your own data and information that is protected in our bill of rights. Our bill of rights is still good no matter what the technology of the day is. Now, my bottom line in this hearing is we've got to find a way to protect and enforce the Bill of Rights and the basic personal liberties of every law-abiding citizen in this country, no matter what the technology is. That I think is the challenge that is facing us today. And I have to tell you based on what these reports are, we've got some work ahead of us.

You know, to give you another example, a customer in a **Flock** network, for example, just needs to buy a single camera and a subscription that I'm told costs about $3,000 annually. And in return for that, they get access to a nationwide database of tens of thousands of cameras, about 120,000 in **Flock's** case, and billions of images. And **Flock** has admitted that until very recently, there were basically no curbs or restrictions on which of these subscribers, so to speak, could search their databases, what they could do with the images, how long the images were kept, or what other uses they were put to. In fact, customers can search using natural language across this data set, including images that are months and months old. **Flock customers are**

even able to assemble a 'pattern of life'—that's a comment from Flock itself—a pattern of life for the millions of vehicles that are caught up in what is becoming a massive drag net.

You know, the overwhelming majority of drivers or other travelers who are surveiled here have done absolutely nothing wrong. Nothing wrong at all. And I think that's what's so troubling to people as they learn about this technology. It sounds as if based on the reports we've heard, it's treating every citizen in America. I mean by now surely almost all of us have been scanned and logged as if we are criminals yet without any due process, without any reasonable suspicion, without any articulable suspicion whatsoever. This just seems very very strange to put it mildly and something I think this committee really needs to hear about.

You know, you're going to hear in just a moment from someone who has suffered at the hands of this surveillance network, **Lindsay Isaacs, who joins us from Palm Coast, Florida. She was falsely accused of being in a car crash causing one in fact and she spent 13 days in jail because of a misidentification from one of these surveillance networks. She's totally innocent.** You're going to hear from **Alistair Whitney who's a legal expert for the Institute for Justice, which is an organization that's been documenting the use and sometimes abuse of these cameras.** You're going to hear from **Sheriff Ross Teeple, who we're so proud is here today from Arizona, who recently decided to terminate his department's use of these cameras in order to protect the privacy of his citizens and to comply with the Constitution of the United States.** You're going to hear from **Ben Jordan, who's a cyber security researcher who's going to speak personally to the very real risk that these cameras can be hacked and all of those images, billions of them, can be accessed by malign actors.** And you're going to hear from **Chad Marlo, who's a senior policy counsel at the ACLU, where he leads their Get the Flock Out campaign.**

Sadly, who you're not going to hear from today are the CEOs of **Flock** and **Axon** and **Motorola** and **Vercada**. I invited all of them as **Senator Durbin** and I did, the whole committee. We sent letters to them and asked them to be here and they're not. And I think that that's unfortunate. I think we need to hear from them about what it is their networks do. I think we need to hear from them about their intentions, about their capabilities, and we need to have an honest conversation about where this is leading us as a country.

I'll close with this and let **Senator Durbin** make his opening remarks. I just want to say this. You know, this is still the United States of America, and it shouldn't be that when you walk out your door in the morning, you just have to agree and ascent and accept the fact that you're going to be on camera morning, noon, and night. You'll be tracked by anybody and everybody in the world. You'll have no privacy whatsoever. You'll be tracked when you take your kids to school and tracked when you go to church and tracked when you go to the grocery store. My gosh, that isn't the free society that we've known. That's not what the Constitution guarantees. We've got

some work to do, I think, to make sure that the Constitution is real and protected in this area. And I look forward to doing it today, getting a start at least. **Senator Durbin**.

Ranking Member Durbin: Senator Hawley, good hearing. Glad to be here and looking forward to the testimony for the **Flock** CEOs. Obviously, they're nervous about being on camera, but I sure wish they would have joined us today. It would have been interesting to hear their explanation of the statistics that have been given us by **Senator Hawley**. 120,000 **Flock** cameras in 49 states. Which state doesn't have them? Hawaii. Hawaii. I wonder why. Maybe we'll learn.

The collection of information and data is what it's all about these days. **Amazon**, I'm told, makes more money off the data that they've collected about their customers than they make off the merchandise that they sell. Hard to imagine, but that information is being sold regularly and collected constantly. And that's what this hearing is all about.

I support law enforcement. I'm glad they're here represented by **Ross Teeple** and others and we entrust them with keeping us safe in our homes and our neighborhoods and our businesses and as we go about our business. But we also value privacy. If you're a constitutional scholar, please tell me where the word privacy is in this constitution. You won't find it. And yet the courts have found the inference of privacy and determinations of things as basic as reproductive choices by couples. So we know that there is some privacy protection.

We also know that as we look at the information that's gathered, it's being gathered for many years. This is nothing new. The volume of the undertaking is new. The state of Illinois has had an **ALPR** automated license plate reader as part of their state effort to catch people on the tollway who don't pay their fair share. This has been around for a long time. It's been used to locate people who've gone missing, cars connected to crimes and stolen vehicles. That all sounds good.

And then you hear the story of **Miss Isaacs** (referred to below as **Lindsay Isaacs**). She'll tell you in detail what she's been through when the so-called failsafe technology fails, and it certainly did in her case. I just want to say to the chairman, thank you for this hearing. We have got to find a way to balance in America privacy and security. I think there is a balance, but Congress needs to lead the way. Thank you, Mr. Chairman.

Chairman Hawley: Thank you very much, **Ranking Member Durbin**. It's the practice of this subcommittee to administer an oath to our witnesses before they testify. So,

---

CHAPTER 2: VICTIM TESTIMONY

Lindsay Isaacs: Good afternoon. My name is **Lindsay Isaacs**. I'd like to share with you what happened to me beginning on October 4th of 2025 and how it forever changed the trajectory of my life. On October 4th, 2025, I spent the day with my mom cooking at my apartment in Palm Coast, Florida. We left my apartment separately at around 6:30 p.m. She drove home to Ocala and I drove to a store in Davenport. It was a normal drive. I stopped for gas and then continued to the store. I stayed at the store for about an hour before heading home. I arrived home at approximately 10:25 p.m. ate some of the food my mother and I cooked earlier that day and called my parents to say good night.

At approximately 10:04 a.m. on October 5th, an **FHP** trooper and three deputies from the **Marion County Sheriff's Office arrived at my parents' home in Ocala looking for me. They asked where I was and where my vehicle was and told my parents that I had been involved in a fatal crash.** My parents were confused and terrified. They told law enforcement I was home asleep in Palm Coast and gave them my address. They could not understand what they were being told, and they were now worried about whether I was even alive.

My parents immediately drove to my apartment. They arrived at approximately 4:45 a.m. and found additional troopers there already. I woke up frantic. My parents were at my door. Multiple troopers were outside and **an impound truck was taking my Dodge Durango away right in front of me.**

I gave the troopers my receipt and information showing where I had been. I told them that I had not been involved in any crash. The troopers told me that there was damage to my vehicle consistent with the collision, but I could not see the damage they were describing. My Durango was in immaculate condition. **Yet, I stood there watching law enforcement take it away while telling me that my vehicle had been involved in a crash where three people died.** The same day, October 5th, 2025, I retained **criminal defense attorney Patrick McGee**. In February of 2026, my defense team sued the **FHP** seeking the return of my vehicle.

I later learned that a Flock automated license plate recognition camera had captured my Dodge Durango approximately 2 to three miles west of the crash scene. Investigators were looking for a black Dodge Durango. I also later learned that the witnesses had described a maroon Dodge Durango as being involved in this crash and that 911 callers provided information about that vehicle, including a partial license plate of 458. Despite this information, the investigation continued to focus on me and my vehicle.

On April 17th, 2026, a warrant was issued for my arrest. I was ordered to surrender myself at the Volusia County Jail by 2 p.m. I could not understand what was happening. I was placed in solitary confinement for approximately 3 and 1/2 days. Correctional officers told me I had to stay there because of the severity of my charges and I could not be housed with other

inmates until I had been evaluated. I was placed in a blue suicide prevention dress with a broken velcro on the left side that left me exposed. The cell door was shut and it was not opened for approximately 86 hours.

I'm sorry. **I was then moved into a mental health unit for approximately 24 hours before ultimately being transferred to GBlock, a maximum security housing unit where I remained for approximately 10 days. I was terrified. I was facing the possibility of spending the rest of my life in prison for a crash I knew that I knew I had not been involved in.** I did not know if I would ever get out of jail. At my lowest point, I didn't want to be alive.

The television was constantly on in the jail. My mugshot appeared on the news and I watched as information about me and my case was broadcasted publicly. Other inmates harassed me about my charges. Every day I prayed that the truth would come out. When another inmate was sent to prison, she gave me her Bible. I read that Bible every day. I slept with it as my pillow. I even took it into the shower because I almost had nothing else and I was afraid someone would take it and steal it. I still have that Bible today and I cherish it.

On April 22nd, 2026, I was denied bond at my pre-trial detention hearing. **On April 28th, my attorney, Patrick McGhian, presented the court with multiple photographs of my Durango sitting in the FHP impound lot without the collision damage investigators had claimed was present. This prompted the state to re-evaluate my vehicle and the case against me. The following day, April 29th, I was finally granted bond. After 13 days in jail, I ran into my mother and father's arms. I could not believe I was free.**

In May 2026, the state ultimately declined to prosecute me and filed a no information and information was never filed against me. The investigation instead resulted in charges against another individual. I came here today because I want you to understand that surveillance technology does not exist in a vacuum. Information collected by technology can become part of an investigation that affects a real human being. **In my case, a Flock camera captured my vehicle a few miles from the scene of a terrible crash. That piece of information became part of an investigation that ultimately led to my arrest on three counts of vehicular homicide and 13 days in jail for a crash I had nothing to do with.**

I'm not here to tell you how to do your jobs. I'm here to tell you what happened to me. Thank you for allowing me to share my story with you today. I thank God, my family, and **my attorney, Patrick McGhian**, for standing beside me and helping me get my life back.

Chairman Hawley: Thank you so much, **Miss Isaacs**. Thank you for being here, for sharing that. Thank you. **Mr. Whitney** is next, **Mr. Alistair Whitney, who serves as legislative counsel for the Institute for Justice**. **Mr. Whitney**, floor is yours.

CHAPTER 3: LEGAL AND CIVIL RIGHTS

Alistair Whitney: Good afternoon. Good afternoon, **Chairman Hawley**, **Ranking Member Durbin**, members of the subcommittee. Thank you so much for inviting me to testify today. My name is **Alistair Whitney** and I'm legislative counsel at the **Institute for Justice**. **IJ** is a nonpartisan public interest law firm that works in both state houses and courthouses around the country to defend your constitutional rights.

ALPR technology now lets the government do something it can never do before, and that is travel back in time and reconstruct your movements, where you've been, and with whom you've associated, all without a warrant and with the ease of running a Google search. Governments say they need this kind of frictionless access to fight crime. And the goal is of course laudable. But as the **Supreme Court** has said, the warrant requirement is not an inconvenience to somehow be weighed against the claims of police efficiency. Technology may make surveillance more convenient, but it does not make the **fourth amendment**'s protections any less important.

Now, most people picture **ALPRs** as a camera that reads a plate, but that picture is roughly a decade out of date. As the chairman mentioned earlier, **modern license plate readers photograph every single car that passes. They never blink. They never sleep. They can record make, model, color, bumper, stickers, dents. They can map everywhere a car has been photographed. They can flag cars that travel together. And they are networked. One vendor alone runs a dense network of more than 120,000 cameras in 49 states and logs 20 billion photographs of vehicles every single month.** This means, of course, that an officer in California or Florida can access information and data showing where somebody has driven in Missouri or Illinois with the ease of a couple of keystrokes or clicks.

No federal law governs any of this and many states don't have any law on the books either. Where rules exist, a vendor often wrote them and they change with a software update or a publication of a missive on a website. The result is what you would come to expect and sadly what we've come to see.

For example, **in Kentucky, an officer allegedly searched a Flock database for his child's mother thousands of times over several months, despite the woman having received an order of protection against him. In North Carolina, an officer was arrested after allegedly accessing Flock's database to look up an undercover investigator's vehicle at the request of a drug suspect. Innocent families have been held at gunpoint over a misread letter on a plate. Images from these cameras have been shipped to gig workers in the Philippines to train Flock's AI. IJ's**

public database now documents hundreds of incidences like these and unfortunately the number of abuses are growing by the day.

The **fourth amendment** has something to say about this. **In Jones, in Carpenter, and this June in the court's decisions in Chatri, the Supreme Court made clear that we do not surrender our constitutional rights when we are in public. In Chatri, 2 hours of location data was enough to require a warrant. Here we are talking about weeks or months.** That is why **IJ** is litigating this warrantless surveillance in two federal courts. **In Norfolk, Virginia, 175 unblinking eyes captured 41 million vehicle images in less than a month. In San Jose, California, the city had four cameras at a single intersection in 2021. Today, just under 500 cameras are across the city, taking hundreds of millions of photographs a year, which more than a thousand city employees and nearly 300 other agencies in the state search roughly 15,000 times a day. Networks that dense let the government track anyone cheaply for weeks at a time.** That is exactly why law enforcement likes them.

Regardless of how these cases turn out, here's the point that matters here the most. **The Fourth Amendment is a floor. It's not a ceiling. Congress** did not wait for the courts on wiretaps or bank records and it should not wait here. Even the judge who ruled against us in Norfolk said that the guardrails should come from **legislators**. This **Congress** should act now.

Congress can require federal agents to get a warrant before they search historical location data as our model legislation does. It can impose tight limits on how long that data is kept and it can condition federal dollars on states and localities doing the same. To be clear, none of these restrictions would stop law enforcement from finding a missing child or a stolen car. We're not asking for you to turn the cameras off with this model legislation. **The warrant requirement is the bare minimum, though. Without it, there is simply no constitutional way to run these systems because they sweep in the overwhelming majority of drivers who have simply done nothing wrong. And what they capture is not just a day in the life, but a way of life.**

This is why Americans opposition to their unchecked spread crosses every single political line, prompting a growing number of cities and states to slam the brakes on this technology. So we urge the honorable members of this subcommittee to enforce constitutionally grounded restrictions on this technology before these cameras end up on every street corner. That is not just concern. That is **Flock's** stated goal. Is that the America that we want to live in and hand to our children? For me personally, the answer is no. Thank you very much for your time and I look forward to your questions.

Chairman Hawley: Thank you, **Mr. Whitney**. Next is **Sheriff Ross Teeple**. It's an honor to have you here, **Sheriff**. **Sheriff Teeple** is from **Pinal County**. Did I get that right? Am I saying that

right? In Arizona. Thank you again for your service and thank you for being here. The floor is yours. It's an honor to serve.

CHAPTER 4: LAW ENFORCEMENT PERSPECTIVE

Sheriff Ross Teeple: Good afternoon, **Chairman Hawley**, **Ranking Member Durbin**, and distinguished members of the subcommittee. Thank you for the invitation to speak before you today on this critical issue. Before I begin, I would like to acknowledge **the passing of Jon Kyl last week. Senator Kyl dedicated his life to serving his country and Arizona.** I extend my deep condolences to his family and his colleagues that worked alongside him here in the Senate.

My name is Ross Teeple and I am honored to be elected the 25th Sheriff of Pinal County, Arizona and proud to be married to my beautiful bride for the last 33 years. Protecting public safety and defending constitutional rights are law enforcement's most important jobs. I am here today because I firmly believe we can use technology to keep our communities safe while still achieving both of these vital goals.

Let me be entirely clear. Automatic license plate readers or **ALPRs** are a great tool. Technology that is strictly limited to reading a license plate helps us solve crimes, catch dangerous criminals, and find missing people. It allows us to cross-reference plates against stolen vehicle databases or respond to active **Amber Alerts** instantly. **Under the Supreme Court's landmark 2020 ruling in Kansas v. Glover, running a license plate to check registration status provides the reasonable suspicion needed to make a proactive traffic stop. Used properly, point in time license plate reading is common sense policing.**

The committee reached out to me because I was one of the first law enforcement leaders in the country to end our contract with Flock. Make no mistake, that decision was controversial, but it was extremely popular on both sides of the political spectrum. **Pinal County** represents unique law enforcement challenges. It's the size of Connecticut, lies between Arizona's two biggest cities, and is about 60 miles from the border. Interstates 10 and 8, some of the busiest human and drug trafficking corridors in America, run right through the heart of my county. There is a good chance that the fentanyl being sold outside Union Station right across the street or in your hometown came through my county. Given those challenges, it would be irresponsible not to equip my deputies with the best technology to help them do their jobs. But I will never allow technology to supersede your rights.

I believe the latest camera networks powered by artificial intelligence and machine learning are capable of violating our citizens' fourth amendment rights. We have entered an area where some camera networks are capable of capturing much more than just a snapshot of a

plate on a highway. If my deputies need a search warrant to put a physical tracker on a vehicle, where is the line for camera systems that build an identical AI-driven map of a citizen's life?

Recently, I received an email from a law enforcement colleague regarding these FA cameras that I found chilling. He wrote, quote, "Some courts compare point in time to continuous tracking as the reasoning. Will there someday be a **Supreme Court** ruling on these? No doubt. But today, as I type this, there is no violation of the **Fourth Amendment**." End quote. With all due respect to my colleague, that is the wrong mindset. **We shouldn't wait for the Supreme Court to tell us something is a violation before we decide to protect the privacy of our citizens.** History has shown us the cost of law enforcement moving faster than the **Supreme Court** constitutional rulings.

60 years ago in my state of Arizona, a detective arrested a man named Ernesto Miranda. The detective got a confession and secured a conviction. But because procedural safeguards weren't actively protected, the **Supreme Court** threw that conviction out in Miranda v. Arizona, fundamentally changing law enforcement forever. Now, everybody in America has heard of their Miranda rights. What people forget or don't know about Miranda rights is that detective should have known better. It was already common practice back then to let suspects know they have a right to remain silent and they have a right to an attorney.

Now, everyone in America has heard the word **flock**, and in **Pinal County**, it's become a four-letter word. **We rely on private camera networks. If we rely on private camera networks to act as a drag net, continuously logging the habits of innocent Americans without a warrant, we are paving the way to an AI-driven surveillance state. If we allow government-funded private surveillance companies to push this envelope blindly, we risk a sweeping judicial correction that could strip away the legitimate life-saving aspects of ALPR technology entirely. We must establish clear statutory boundaries for automatic license plate readers. We cannot wait for a future Supreme Court ruling to correct AI overreach. We must protect the Fourth Amendment today.** Thank you and I look forward to your questions.

Chairman Hawley: Thank you very much, **Sheriff**. Thank you again for being here. Next up is **Mr. Ben Jordan**. **Mr. Jordan** is a cyber security researcher with extensive experience investigating the surveillance networks, **Flock** in particular, as well as its peer companies. **Mr. Jordan**, thank you for being here. The floor is yours. Thank you for having me.

CHAPTER 5: CYBERSECURITY AND RISKS

Ben Jordan: Um, as the Senator just mentioned, **I'm an independently funded cyber security researcher**. So, I don't really work for a company or anything to do so. Um, I sort of do so as my own my own hobby that is then funded through a **YouTube channel** and **Patreon** and stuff like that. And that's a nice way of saying **I'm a hacker**.

Over the summer of 2025, I started learning about some of the weaknesses and the security and the efficacy of the **ALPR** industry's ecosystem in hardware. I found that **flock** at the time did not require their clients to use multifactor authentication. This led me to find **flock** law enforcement accounts for sale by a **Russian vendor on a dark web** marketplace which was referenced in **Senator Wyden and Representative Krishnamoorthi's letter urging the FTC to investigate Flock as a national security risk in November of 2025**.

I then met and worked with **John Gaines who had discovered, detailed, and published 55 security vulnerabilities related to Flock**. **Some of these vulnerabilities are published through MITRE, who manages security vulnerabilities for the Department of Homeland Security**. The most alarming of **John Gaines**'s reported vulnerabilities was in the most common model of **Flock's ALPR** camera. I publicly demonstrated that by pushing the button on the camera three times, **I was able to access all of the data or reprogram the device however I wanted in under a minute. A back door, malware, I even played Doom on a Flock camera**.

In addition to this, **John Gaines** and myself found insufficiently protected sensitive information stored on **Flock** cameras, including photos, license plate data, logs, API keys, passwords, and communications. Then in December of 2025, through a specialized search engine, I found the unprotected administrative interfaces for over 60 newly deployed **Flock** Condor cameras that had AI enabled pan, tilt, zoom features. **This allowed me to remotely view, delete, and modify 30 days of streaming footage from the cameras across the country and potentially sensitive locations like forest trails, people's front porches, and playgrounds. And I could also zoom in on people's mobile phone screens**.

Another security researcher, Joshua Michael, independently found a misconfigured flock development demo via a Google search that included ArcGIS API keys with virtually unlimited usage limits. ArcGIS stores enormous amounts of data from local governments ranging from the live GPS location of police vehicles to aerial drone feeds.

Flock has over the last year repeatedly claimed that their service utilizes end-to-end encryption. Both **John Gaines** and myself have verified the lack of end-to-end encryption in a variety of different ways. **But the most alarming consequence of this was in Dunwoody, Georgia, where FOIA requests showed that flock employees had viewed cameras on their network over a thousand times, including the ones in sensitive areas like the interior of a Jewish community center and a playground**.

Flock's response to my videos over the past year and media stories about our research had primarily been defensive or in denial of the many reported vulnerabilities. But in light of recent events, they have invited myself and other researchers to review their hardware and platform. And while there hasn't been enough time for a thorough review before this hearing, I can testify that in my opinion, it does appear that they're taking security a lot more seriously than they were a year ago.

I have been one of **Flock's** harshest critics for years. But everything that I just stated about them is a symptom of a much larger problem in my opinion. What I've been asking for around the country is for privatized government surveillance vendors to require independent security testing and inspections. **I cannot legally open a restaurant or a barber shop without a health inspector and a fire marshal making sure that it's safe for people to enter. Yet, there is not a single city or police department in this country that requires this from a third-party company tracking their citizens**.

I want to use my time here to ask our legislators to take this rare bipartisan agreement they're having to view Flock as a canary in the coal mine and understand that this doesn't go away by just removing one company from the equation. Both Axon and Motorola are actively rolling out the same reckless features that we're shaming Flock for. And you can expect these same vulnerabilities will continue to happen over and over again when innocent people's data is traded between private companies and police without any safeguard or protection.

Some members of this community are in support of the **Combating Organized Retail Crime Act**, which has broad definitions that could lower the security posture of sensitive civilian data to the standards used by retailers. After reading that bill, I immediately imagine the scenario where **Home Depot** or **Target** with their data breaches affected hundreds of millions of Americans, but now I'm imagining them also including their location data and sensitive information related to ongoing investigations.

So to be as concise as possible from a security perspective, it would be absurd to be concerned with the scenarios playing out with Flock while supporting bills like CORCA or the extension of FISA Section 702. That would be the equivalent of feeding a monster in an attempt to defeat it.

ALPRs are used all over the world, but viewing license plates as personal data with modern privacy guard rails would have prevented nearly every single problem that we're learning about in this hearing. This is an opportunity for **Congress** to build the overdue framework to protect the privacy of Americans for generations to come. Thank you.

Chairman Hawley: Thank you very much, **Mr. Jordan**. Finally, **Mr. Chad Marlo**. **Mr. Marlo** is senior policy counsel at the **ACLU**. **Mr. Marlo**, thank you for being here. Floor is yours.

CHAPTER 6: ADVOCACY AND POLICY

Chad Marlo: Chairman Hawley, **Ranking Member Durbin**, members of the Senate Judiciary Subcommittee on Crime and Counterterrorism. On behalf of the **American Civil Liberties Union**, I want to thank you for the privilege of testifying before you today. My name is **Chad Marlo and for the past 12 years I have served as a senior policy counsel at the ACLU where my work focuses on surveillance, privacy, and technology issues. In that role, I lead the ACLU's policy and advocacy work on automatic license plate readers or ALPRs, including the ACLU's Get the Flock Out campaign.**

I want to begin my testimony by answering the question I think is on the mind of every person in America. Namely, how did a country founded upon principles of liberty, personal freedom, and inalienable rights, including the right to privacy, find its people's vehicular locations and movements being tracked by governments at the local, state, and federal levels, even though virtually none of us are suspected of committing a crime. Put more succinctly, how did we get here?

As you know, **ALPRs** are not new technology. They have been in use in America since the late 1990s. So why then in the last several years have we seen an explosion in **ALPR** use and its tracking of innocent people? The answer is twofold.

The first is the entry of venture capitalist funding into the mass surveillance industry. Let me be clear, these massive investments do not reflect a rise in venture capitalist interest in public safety. Rather, it reflects a view that **ALPR** use, if scaled up, could produce the massive profits venture capitalists seek. But to achieve such returns, the **ALPR** industry needed to go bigger, much bigger. And that meant pushing far greater **ALPR** deployment, tracking, data retention, and data sharing to produce far greater profits. In short, **ALPR** companies are in the business of trading our privacy for profits, and they are getting rich off of it. Welcome to the surveillance industrial complex, America.

The second cause of the spike in **ALPR** use is the advent of artificial intelligence. While the massive deployment of **ALPRs** allows for the collection of an unimaginable amount of location data, at some point you create a data haystack so big it becomes impossible to find the needle within it. But with the advent of AI, going through billions of **ALPR** scans and using them to identify drivers' intimate patterns of life—like what doctor's offices, religious institutions, political meetings, or businesses a person frequents—and even using the AI to generate flimsy criminal suspicion has become light work.

Because **ALPR** systems are most commonly sold to local police departments, a nationwide **ALPR** surveillance network crept up on us slowly and silently until it was too big not to notice. In early 2022, the **ACLU** became the first organization to sound the alarm about this emerging threat as embodied by **Flock** Safety's **ALPRs** on steroids business model. The rest of America soon joined us and here we are today.

Flock safety **ALPRs** collect more than 20 billion license plate scans per month. That's 57 scans per person in America every month. And that's just **Flock**. If you think that sounds like an Orwellian nightmare, you'd be right.

Beyond revealing intimate patterns of life and generating questionable suspicion, the most concerning impact of **ALPR** mass surveillance is that it can chill the exercise of people's rights and freedoms. This is why authoritarians love surveillance. In places like Cold War East Germany and modern-day China, the main benefit of mass surveillance isn't catching the few people who break the law, but rather putting all their people in fear of stepping out of line with the government's interests. That is the chilling effect, and it's coming to America.

In 1755, Benjamin Franklin wrote that those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety. While that is certainly true, today's situation with **ALPRs** is even worse because the people are being asked to give up their privacy for virtually nothing in return. Decades of studies demonstrate that surveillance does not deter crime outside of its use in public parking lots and on public transportation. So, we get no public safety benefits from **ALPRs** there.

Moreover, a recent study of **FBI** crime data for Atlanta shows that the deployment of more than 5,000 **ALPRs** in that city had no effect on case closure rates. What that means is that where an **ALPR** identified a stolen vehicle or a wanted person, that vehicle or person would have been found anyway. Yes, perhaps the **ALPR** would have found the person a few hours or days faster, but that marginal gain does not justify undermining the privacy of 350 million Americans.

Because of all this, nonpartisan opposition to **Flock**, **ALPRs**, and mass surveillance has reunited America in 2026, and our leaders are listening. Vermont banned the use of **ALPRs** effective July 1st, 2027. The governors of Texas and Florida have taken strong executive action to prevent the funding and deployment of **ALPRs** in their states. Locally, more than 200 municipalities have terminated their relationships with **Flock** and other **ALPR** companies.

The question is, will their **Congress** join them? The time has come for **Congress** to prohibit any law enforcement entity who receives federal funding from using **ALPRs** without exception. Because when it comes to protecting civil rights and civil liberties, if you make one exception, you invite others. And that is a slippery slope we must avoid at all costs. So I implore you senators to be brave and unrelenting in responding to these mass surveillance threats. And

please know with absolute confidence that the **ACLU** and the American people stand behind you. Thank you for the opportunity to testify. I look forward to answering your questions.

Chairman Hawley: Thank you very much, **Mr. Marlo**, and to all of the witnesses. Now, we'll start some rounds of questioning.

CHAPTER 7: COMMITTEE QUESTIONING *(SUPPLEMENTAL SUMMARY)*

During the cross-examination period, **Mr. Chad Marlo** of the **ACLU** famously addressed the legal data loopholes exploited by immigration agencies like ICE via local police departments by firmly telling **Senator Padilla**, **"You ban them, sir. You ban them."**

Parallel to this, cybersecurity researcher **Mr. Ben Jordan** detailed that software and administrative protections are effectively minor caulking fixes over massive gaps. He highlighted that even if companies enforce rigorous localized safeguards, the core issue is the systemic exposure of immense volumes of raw tracking data, stating that trying to lock down a platform creating this much information is like standing in a 30,000-foot warehouse trying to stomp out ants with a single shoe—ultimately, access remains entirely up to the attackers.

CHAPTER 7: COMMITTEE QUESTIONING

Chairman Hawley: Now, we'll start some rounds of questioning and I'll begin and I want to start with you, **Mr. Alistair Whitney**, if I could and help me and everybody watching understand what's the difference between this technology that we're talking about today, this AI powered technology and a traditional license plate reader technology. And here's why I ask. I'm a former prosecutor. We've got **Senator Richard Blumenthal** is a former prosecutor. I think **Senator Amy Klobuchar** is a former prosecutor. Yeah, that's right. I'm sorry, I should have started with you, **Senator Amy Klobuchar**, my mistake. This is common and when I was attorney general of Missouri, we used license plate readers all the time. **Sheriff Ross Teeple**, I'm sure you use them constantly. I mean, the very familiar technology. However, my understanding is what we're talking about here today with this linked network of private cameras all uploading to the cloud, searchable and powered by AI is something very different. So, explain that to us if you could. What's the difference? Why is this a qualitatively different kind of technology?

Alistair Whitney: Well, thank you for the question, **Mr. Chairman**. You said it. The fact that this technology is now interlinked with cameras across the country in this network that allows a government official or an officer in one side of the country, say California, reconstruct the past movements over weeks or even months of somebody driving in Maryland or Virginia, is

something that is both qualitatively and quantitatively different than a technology that we've ever seen before. And that is why we are concerned about this and what makes it different from the **ALPRs** of yesteryear.

Law enforcement can do this right now, as I said, with the ease of conducting a Google search, right? And then they can get this information showing where you've been, what you've done. In our San Jose litigation, for example, we've seen these cameras placed in front of attorney's offices, medical facilities, churches, mosques, other places of worship. And to allow government officials all over the country to access that information and potentially track where somebody has been going and what they've been doing is concerning.

And of course, this is all supercharged by AI. A couple of years ago, you couldn't possibly sift through 20 billion images with just a few officers or even 100 or a thousand officers. But AI now makes it much easier to do that with again a click of a button or a couple of keystrokes.

Chairman Hawley: If you just to pick up on that point, if you have hundreds of billions of images now that are being collected and collated and available in the cloud and you've got AI able to search them, you really can reconstruct or the AI can reconstruct the very granular movements of individuals over long periods of time. Isn't that right? I mean, they could track me driving from Missouri out here, taking my kids to school, going to church, doing everything that it is that I do. And you could do it for days and weeks at a time using this vast network. I mean am I exaggerating? Is that right?

Alistair Whitney: No sir, you are not exaggerating and that is exactly right. I mean the again we've heard for the proponents of this technology and using it in a way that they've been using it right now that you know that they don't use it to track people. I think that that's just simply untrue. The value of this technology is tracking people and is determining where they are and what they've been doing, including sometimes images of the person, right? Facial images.

Chairman Hawley: Let me just put up a poster here. Poster number nine, guys. **ALPR** does not use facial recognition as a claim we often hear from these companies. And of course, traditional license plate readers don't track individuals at all. I mean, that would have no purpose, right, **Sheriff Ross Teeple**? I mean, you're trying to get the license plate so you can run the chain of custody on the car, see the driver's license. It doesn't track individuals. But we now have, we know this technology is now able to track facial recognition despite what they say.

And you can see it on the poster of the motorcycle. Let's take a look at this that I showed earlier. This is from a **Flock** camera, I believe. Look, it's already the analysis of the **Flock** camera is already saying there's the license plates, there's the vehicle, and there's the person. So, it's separating out the person and this image would be totally searchable in this nationwide database. We also know that **Flock** has applied for a patent that would permit the tracking of

individuals. They call it a patent for a dynamic surveillance network that would allow searches of individual persons by image in this huge database. I mean, this seems to me to be something unlike anything we've seen before. Am I right about that, **Mr. Alistair Whitney**? I mean, we're a long way from a traditional license plate reader here.

Alistair Whitney: Yeah, absolutely. And what we have seen obviously with the information that you've shown today that these surveillance platforms—and that's really how they should be more accurately described—are capable of course with a click of a button of being enhanced with software to perhaps do this one day. And I will note that in the images that we just saw, if there are other motorists, motorcyclists around, or pedestrians, the camera is capturing images of those individuals as well. So it's all very concerning.

Chairman Hawley: The **Flock** CEO wrote me a letter in response to my invitation to testify today. And in that letter rather, the CEO said some interesting things. And I just want to put these on the record to make sure that we all understand what we're talking about here. **Flock** acknowledged that it conducts very little oversight of client searches and instead relies on its clients to police themselves and said, and I quote, *"Now, the underlying search records are owned and controlled by each customer agency."* So in other words, once you subscribe, you've got access to the whole database.

Flock clients control the data retention. So these images, billions and billions of images a month, have not been set to expire, not been set to be expunged. Until last year, **Flock** customers could enter the reason for a search into a free text field, that's their words, which did not have any meaningful accountability. And we know that various persons entered their reasons for searching into the database to include terms like the reason was just *"search"* or the reason was *"lol."* I mean no cop would do that, right?

I mean **Sheriff Ross Teeple**, you can attest to this and we'll come back to this here in a minute that when cops use license plate readers, and I want to say I think that's very valuable technology, but only a certain number of law enforcement agents have access to that technology. You got to log a reason for using it. You've got a law enforcement purpose. I mean, this is how we do it in Missouri. It doesn't appear to me that that's how these **Flock** cameras and others are being used. I mean, they're just open to just about anybody who subscribes. There are no controls on them put by the companies. And **Flock** also admitted in their letter that it is possible to search for humans in images. That is a direct quote. Let me say that again. It is possible to search for humans in images taken by **Flock** cameras. That's currently today. That is possible. And again, all powered by AI. This just seems very concerning. Much more on this to come. **Senator Durbin**.

Ranking Member Durbin: I'd like to ask **Mr. Chad Marlo**. We are concerned in Illinois with Operation Midway Blitz where **ICE** and the **Department of Homeland Security** came into our state and started looking for people to deport. They ended up deporting a substantial number. And it turns out that their promise to limit those deportations to the worst of the worst, as the president characterizes—the rapists, murderers, terrorists, sexual predators—turned out that the majority of people they were deporting were American citizens not guilty of any crimes. Our state passed a law which limits law enforcement from using **Flock** data for immigration purposes. Have you heard of such laws in other states?

Chad Marlo: Yes, thank you for your question, **Senator Durbin**. So, I have heard of laws like that in other states and I believe that they constitute a good faith effort to protect vulnerable populations. But unfortunately, the news I have to share is the value of those laws is limited. If the federal government, you give an example of **ICE**, were to show up with a judicial warrant or an administrative subpoena for that data, it would not matter much what Illinois law said about it. It would have to be turned over.

If they participate in a data sharing database where just one officer in the state of Illinois is sympathetic to whoever it is is trying to access that data, be it **ICE** or anyone else, they have the ability to run a search on someone else's behalf. And looking at it in the immigration context is horrifying, but they've done the same to people who go to gun ranges. This really is nonpartisan. It is come up with the group you want to target, and with this level of technology, targeting them is fairly easy. So, that is the challenge here.

Ranking Member Durbin: Mr. Alistair Whitney, I heard your testimony saying the answer is a warrant. And a warrant is certainly recognized under our constitution as a valid use of government power authority if used properly. Is that the problem here? The bottom line is they collect the information before there's any specific allegation that wrongdoing has taken place.

Alistair Whitney: Thank you for the question, **Senator Durbin**. I think the problem is collection one, but also the just frankly in most places limitless access to that information without a warrant. **IJ** didn't write the rules. We didn't write the rules. The framers of the constitution did. And they said that whenever you want to search a person in the context of modern technology, this is what a search looks like. You must obtain a warrant.

Ranking Member Durbin: Sheriff Ross Teeple, what was the breaking point for you? You used this information and then decided that there was just too much of a violation of the **Fourth Amendment**. Where did you break with the precedent that had been set before you?

Sheriff Ross Teeple: Senator Durbin, thank you for the question. I'm old. This is the second time I've heard the word **Patreon** here and I don't even know what that is. But that being said, I was the lieutenant over aviation and search and rescue until I was elected to be the 25th sheriff. I

took office January of 2025. My knowledge of **ALPRs** were 20 years old when I worked Stone Garden where they would be mounted on my vehicle and I would see them passing. And then I started getting questions from my constituents and they were asking very specific questions and I started asking **Flock** the company questions and they were not getting answers to me.

I think it's remarkable that **Chairman Hawley** got them to admit that they now can track a person because what I received from a **Flock** representative was I was told our cameras don't take a high enough resolution picture to be able to recognize a person. And when they told me that, I'm looking at **Flock** camera pictures where I could recognize the person on the camera. They had taken a picture, but that was their claim was their cameras didn't take enough and there was just too much disinformation from them and dishonesty. I was trying to get answers from them and they would not give me the answers to them and there were too many concerns. So, we just decided not to continue our contract.

Ranking Member Durbin: Thank you for raising that point because it's not a matter of just reading license plates that seem so routine, but it comes to the point where you can identify and recognize the people in the car. You can imagine in a state like Illinois and your state as well, the Hispanic population views this as a threat to their existence where they can be pulled over for driving while looking Hispanic. And unfortunately, we've seen too many instances where people with no criminal records, American citizens, removed from their homes and arrested and deported. It's just the kind of thing that's hard, if not impossible, to explain. I want to give a minute to **Miss Lindsay Isaacs** here. When I listened to your description of your experience, the thing that struck me was whatever the law enforcement agency involved there had tangible evidence in your car that could be viewed. I mean, did you take a look at it later and see the damage that they were referring to?

Lindsay Isaacs: Thank you for your question, **Senator Durbin**. There was no damage on my car at all. That car was a brand new vehicle. I got it with zero miles on it. And when they took the car, it didn't even have 10,000 miles on it. It was in perfect condition and they still said there was damage consistent with the collision on the vehicle. I don't understand that.

Ranking Member Durbin: If the notion here is to gather accurate information so we don't make the mistake that led up to your incarceration, yeah, there was a failure here, a complete failure. So, a misuse of the information. Sorry for what you went through and thanks for your courage in testifying.

Lindsay Isaacs: Thank you so much.

Chairman Hawley: Senator Katie Britt.

Senator Katie Britt: Thank you so much, **Mr. Chairman**, for putting together this hearing and for everyone taking time to be here today. Obviously, this is an important topic and it's received a great deal of public attention in the last couple of weeks and debate and very much warranted. I think two things can be true at the same time. One, we want to keep and make sure that our law enforcement officers have what they need to keep Americans safe to help make sure that, you know, children who have been abducted get home, but we must protect people's **Fourth Amendment** rights. And when we're looking at this, I want to make sure that we're kind of looking at the total picture.

Senator Mark Warner and I came together and wrote a letter. And **Mr. Chairman**, I'd like to ask unanimous consent that this be submitted for the record. Thank you. We talked about our great concern over the widespread reports that there was misuse regarding these automatic license plate readers. In here, we talk about many of the good things that we think have resulted, but ultimately believe that appropriate safeguards are necessary to protect against the unauthorized access and abuse that has come to light.

Sheriff Ross Teeple, I'd like to start with you. When we're looking at cases in Alabama, we kind of dug in and took a look at what we were seeing there. We saw that there were missing children, endangered persons, runaway kidnappings, that this has helped locate that person and bring them home. Also, more recently, someone an older adult with dementia and ultimately getting them home. However, you know, we've seen misuse and abuse in Alabama as well. When we're looking at this emerging technology, you know, we want to make sure that we get this right. Can you first talk about some of you you've obviously had access to this, have used it prior to recently. Can you highlight what you believe would be some legitimate uses of this technology and maybe something anecdotally that you've seen it help actually solved with regards to safety and security of the people that you serve?

Sheriff Ross Teeple: Senator Katie Britt, thank you for the question. One thing I'd like to respond is the **National Sheriff's Association** and the **Major County Sheriff's Association** recently published guidelines September 15th of 2026. And I've read through those guidelines and I think that they're an amazing step in establishing those. I'd like to be clear on the fact that I have absolutely no indication or belief that my deputies did anything wrong. My deputies were using the technology correctly. What our concern was is we knew what access we could get from it. We could put a license plate in there, a license plate number or a partial license plate and then find matches. The best one that I can give you most recently, unfortunately, was in my county. There was an aggressive driver that rammed a young lady's vehicle and pushed her into oncoming traffic and she died, unfortunately, and we found him because of an automatic license plate reader.

Senator Katie Britt: When you talked about some of those safeguards that you saw in this letter with the **National Sheriff's Association**, can you talk about what some of those may be that you feel like can help make sure that this is being used the right way?

Sheriff Ross Teeple: Yes, ma'am. One of the biggest ones you can read right in there is taking still images of license plates, not live streaming, not taking video, taking still images of license plates for use of that data alone. Another one is that there should be if I access a **CJIS** information incorrectly in Arizona, it's a class 6 felony. I don't know a law enforcement official that doesn't think that the same penalty should apply if you access this data incorrectly.

Senator Katie Britt: I think when you're looking to some of the reports that we've heard about people, whether it's domestic violence victims, whether it's gun owners, everything in between, this technology being utilized to harass and or track someone is absolutely completely unacceptable. We've got to figure out how we can do this the right way. And based on your experience from what you're telling me, there are some guidelines, there are some things that we could be doing that we're not doing now that we could demand that would ensure that one of the things that we've talked about in this letter and that I hope, **Mr. Chair**, I hope you get an opportunity to look at it, is making sure that the **DOJ** does its part in all of this. We've asked for the proper oversight, the proper guidance, and we hope that state and local law enforcement officers will get that because something has to be done here.

Miss Lindsay Isaacs, I just want to say thank you so much for telling your story. Elevating your voice in any arena is challenging. When you do it on a national stage like this, it comes with a great deal of both courage and conviction. So, I appreciate you doing that and telling your story so that others don't have to go through what you did. And I'm so sorry for all that you endured.

Lindsay Isaacs: Thank you so much. That means a lot to me. Thank you.

Senator Katie Britt: Thank you, **Mr. Chairman**.

Chairman Hawley: Thank you, **Senator Katie Britt**. **Senator Alex Padilla**.

Senator Alex Padilla: Thank you, **Mr. Chairman**. And I, as well, **Miss Lindsay Isaacs**, want to say my heart goes out to you and appreciate you being here today and your willingness to share your story, hoping something good comes out of this going forward. My first question is for **Mr. Chad Marlo**. Part of the conversation we've had here today is not just what does the federal law say or not say, state law, what does state law say or not say, even local laws that can address some of the concerns here, but the use of this technology is also different: federal government use, state government use, local government use, let alone private sector use of the technology. Can you just at a high level kind of break down maybe some distinct concerns between federal government use, state government use, local government use, and private sector use?

Chad Marlo: Yeah, thank you for your question, **Senator Alex Padilla**. I mean, I have concerns about all of the potential uses of this and as an introduction to answering your question, and I appreciate what the committee is doing today. You know, a lot of times we frame these questions as a balance between public safety and privacy. I would like to suggest that this technology is the threat to public safety, it is not a solution to it.

How it is used really depends on different levels. I think the largest use of this technology occurs on the local level. That makes a lot of sense, right? Tens of thousands of local police departments using it and how they use it and how they choose to use it really varies from department to department, which is why the inconsistency in and of itself is a problem. You can adopt rules on the local level, but again, as you drive through a particular state you could experience 50 different sets of rules governing you. So states have stepped up recently.

What's very interesting to me is a year ago, a lot of the states, and I work in practically all of them, were talking about guardrails as being the best thing it could possibly do to reign in this technology. The problem with those guardrails, whether they apply to state actors, federal actors, local actors, there's a couple of problems with them. One, when I look at them, I try to write the best guardrails I can, and I can never close the holes. And if I can see the holes, other people can see them as well. I think that's a major problem.

The other thing with the guardrails is actually there's two other things. One, we know that people don't always follow guardrails. So, you create an attractive nuisance and people are going to be drawn to that nuisance like a moth to a flame. And I think that that's something we also just have to be attentive to that they're not always followed. I also think the final problem is even if you pass guardrails that attempt to strike a balance, when the public sees a **Flock** camera, they drive by their third **Flock** camera in a day, they may not have a copy of the applicable statutory law in their pocket and go, *"Oh, shoo. Data retention and data sharing limitations are better."* Even if they have it, they may not have the confidence they're being followed.

Now we have the chilling effect on the federal level because the last question you asked we see it for immigration enforcement. But the idea that we need to have in our mind because this is bipartisan, thank you and let it stay that way, is the threat presented by the federal government today could be different tomorrow, could be different next year, the next year, and I think everyone on this panel understands that, which is why you have joined together. It's not about the current threat, it's about the ever-existing threat. Right? **George Orwell** wrote about 1984, but lo and behold, it also applies in 2026.

Senator Alex Padilla: So, I appreciate that and you know, good high-level framework of concerns that I think on a bipartisan basis we are trying to tackle. I do want to follow up on one

specific use at the federal level and in some ways it's a follow-up to a question from **Senator Durbin** earlier in the hearing. Broad data sharing with **ICE**. Is it happening or is it not happening? **Flock** claims that it does not partner with **ICE** and that **ICE** does not have direct access to **Flock** cameras or their systems or their data. But we know that **ICE** is still able to access **Flock** data through state and local law enforcement agencies that have entered into cooperative agreements with **ICE** known as **287G agreements**. So, can you explain in more detail how these agreements can function as a loophole for **ICE** or other immigration enforcement agencies to access data that they otherwise couldn't?

Chad Marlo: Yeah, thank you, **Senator Alex Padilla**. That's a great question. So, you actually quoted from **Flock** themselves, which I think shows the problem. First of all, I would point out **Flock** seems to change its story from week to week. It's hard to even run, but they did say for a long period of time that **ICE** does not have direct access to **Flock** data, and that was true. But the key word there is *direct*. Exactly. And so it doesn't even take a **287g agreement**, although that's obviously a major problem. All it takes is one officer in one department who is a customer of **Flock** and participates in their nationwide data sharing program and you get a call from be it **ICE** or any other federal agency that says, *"Hey, can you run a search for me?"* And either because they believe in the cause that that federal agency is pursuing or they just want to be on good terms with them because they may need something from them tomorrow, they say happy to help. And **Flock** never acknowledges that no security procedures it's put in place do anything to protect against the misuse of its system.

Senator Alex Padilla: The question becomes, how do we close that loophole?

Chad Marlo: "You ban them, sir. You ban them."

Senator Alex Padilla: Thank you, **Senator Richard Blumenthal**.

Senator Richard Blumenthal: Thank you, **Mr. Chairman**, and thank you for having this hearing, which I think responds to a strongly felt need all across the country in Connecticut. Literally, this issue is on the front pages of newspapers almost every day with different communities reaching different conclusions and therefore individual rights potentially varying in 169 different towns. And so there is a need for some uniformity in protecting rights and liberties, most especially against surveillance.

Connecticut adopted a law, **Senate Bill 397**, which was signed into statute in May of 2026 just this year, which establishes some restrictions on the use of data. For example, it can't be shared with other states unless there are guarantees of protecting privacy. It can't be shared with a national database, any multi-state or national data sharing system, unless there's written authorization and possibly a warrant. So I am wondering whether states really maybe will offer more protection than **Congress** and whether we can rely on states to fill the gap that exists right

now. Of course, Connecticut's law requires that there be no retention beyond 21 days, which is way beyond the two hours that your organization, **Mr. Alistair Whitney**, would recommend. And the model statute you provided requires a warrant. Would you advocate that there be a federal law that requires a warrant in every instance? Seems to me that there might be objections in some states to that requirement. Would you preempt state statutes?

Alistair Whitney: Thank you for the question, **Senator Richard Blumenthal**. I think ideally the warrant requirement would be first in line with making sure that federal agents are obtaining a warrant before accessing this information. I want to be very clear too there are numerous exceptions to the warrant requirement in emergencies: to prevent the destruction of evidence, to find kidnapped children, stolen cars, when the person consents to their information being searched, things like that. So we're not recommending a complete, you know, horse-blinder review: you must get a warrant in all situations. The **fourth amendment** has never required that and the **Supreme Court's** interpretation of the **fourth amendment** has never required that, too. But I think the federal government has some unique levers that it can pull to get states and encourage compliance with federal grant money, things of that nature.

And ideally, I mean, we do see a patchwork right now, as **Mr. Chad Marlo** noted, in some of these states. I work in many of these states as well, but as we all know, you travel very frequently, at least I do. I'm in Chicago, I travel into Indiana and Michigan very frequently. I would hope that my rights are respected in those places just like they would be respected in my home state and that's where the federal government can come in and encourage these best practices and require it for federal officials.

Senator Richard Blumenthal: To what extent is the, I guess it's kind of a side-door issue, federal authorities using state law or vice versa? To what extent is that a problem?

Alistair Whitney: It's a big problem, **Senator Richard Blumenthal**. In our San Jose litigation, we have discovered that federal agencies on 20 different instances have obtained access to San Jose's **ALPR** data and state law expressly forbids that. So, we've seen that also, I believe, in Virginia where, despite a law that looks actually in some respects pretty similar to Connecticut's law, law enforcement agencies in that state are simply not complying with it. And so, all of this just funnels back to this front-end gatekeeping protection with the warrant requirement because without that, it is a self-executing enforcement mechanism. Without that, it's easy to abuse the system to get that side-door or back-door access.

Senator Richard Blumenthal: And on the retention issue, I can see circumstances or reasons that the retention period should be longer than just 2 hours. Connecticut again is 21 days. Is there real harm done by that kind of more lengthy retention period?

Alistair Whitney: Yeah, absolutely. And just to clarify, first thing, **Senator Richard Blumenthal**, is that our recommended retention period as reflected in our PEEPS act is seven days, right? And we want to make sure that law enforcement ideally has the time to get a warrant and to keep that data and do it the right way, particularly in places where distances or lack of reception and internet access can make that difficult. But I think the problem with anything longer than a 7-day retention, or a short retention period really frankly for that matter, is that in most places 30 days' worth of data on 99% of people who are probably indisputably innocent and not suspected of any wrongdoing—we think that it is a problem that the government just houses this information on all those people just in case.

Senator Richard Blumenthal: Thank you. Thanks, **Senator Cory Booker**.

Senator Cory Booker: Thank you very much, **Chairman Hawley**. **Sheriff Ross Teeple**, I just really enjoyed and appreciate your testimony. I didn't expect to feel such a kinship with you in the sense that I was a mayor 20 years ago. This technology was not in existence then, but I remember going to community meetings where people who had problems with crime and drug traffic in their communities would ask me, *"please, can you put up a camera here to make us safer?"* And we invested in **ShotSpotter**, I'm sure you know that technology, to be able to respond quickly, and it helped us to get people to hospitals who were gunshot victims and more. But what has happened over the last 20 years is stunning. And I just want to ask you really quickly one more time: you went from an understanding that this was a law enforcement tool to help keep people safer, to now you seem to be very concerned about fundamental civil rights because of the massive advancement of this technology. Correct?

Sheriff Ross Teeple: Senator Cory Booker, it's actually good to see you again, sir. We used to own a condo at 111 Market Street in Newark, New Jersey, and I met you very many years ago, sir.

Senator Cory Booker: Forgive me for not remembering.

Sheriff Ross Teeple: No, you would not remember me at all, sir. But when you walked in, I remembered you. I'm blown away by that, sir. Yes, sir.

Senator Cory Booker: I'm blown away. I hope I was nice back then.

Sheriff Ross Teeple: Yes, sir. You were extremely nice. Okay, good, good. And we've since sold the condo.

Senator Cory Booker: I hope you made a profit.

Sheriff Ross Teeple: My beautiful wife works for **United Airlines** and she just transferred out to the San Francisco base, so that's why we sold it.

Senator Cory Booker: Yeah, we have a lot of flight attendants that are in Newark. Yes, sir. Thank you, sir. To my question, yeah, please tell me about your evolution.

Sheriff Ross Teeple: So one of the points I wanted to make that I forgot about earlier is I know my IT director always gives me a hard time about this when I say that AI is recent. He said that AI started to be created in 1956 with a protocol, but artificial intelligence the way we know it didn't happen until **ChatGPT** and **Grok AI** and those sort of things. The contracts that the **Pinal County Sheriff's Office** had with **Flock** were actually signed before AI became a thing. So that was one of my questions I explained to this gentleman earlier before the hearing started: I asked **Flock**, *"What type of AI do you have on your cameras?"* Their initial response to me was, *"Oh, we don't use artificial intelligence on our cameras."*

Then I think it was about two months later, they put out a press release talking about how they use artificial intelligence to create a digital fingerprint of your vehicle. And so I reached back out to them and I said, *"Wait a minute. You told me there was no AI in your cameras."* And the response was chilling to me. They said, *"There wasn't the AI that you were asking about."* I didn't ask about a specific AI. I asked about what was in your camera. So that was a concern for me and you see these advances in technology obviously as an infringement on potential fundamental civil rights.

Senator Cory Booker: It can definitely be an infringement on potential fundamental civil rights. And so **Mr. Chad Marlo**, may I switch to you if I can. Despite the fact that you have an obnoxious amount of hair on your head, sir, I deeply apologize. I feel very inadequate, sir. From the freedom of the press to second amendment rights, we see how authoritarian countries like China arguably use this technology to repress human rights, and I want to just throw out for you to give me some example of this. If a state has a law that prevents a woman from getting reproductive rights, and we're seeing this now where they pass laws about people leaving their state to access reproductive care, a state could be using this technology to track and ultimately, when they return home, prosecute women who are accessing reproductive care. Is that correct?

Chad Marlo: Unfortunately, that is completely correct, **Senator Cory Booker**. And the thing that is even more disturbing about it, we've talked a lot about AI here today. In **George Orwell's** book, even though **George Orwell** didn't know it, Big Brother was never a person. It was AI. And so, you can literally prompt AI to say, *"I want to find people who are leaving my state and seeking abortion care somewhere else where it remains legal."* And the AI will look and they will find the **Planned Parenthood** clinics and they will find the major highways. They will identify the bridges. They will look for patterns: who went to a doctor and then to a drugstore in the state and then returned to the state where it was illegal.

Senator Cory Booker: So just my time is expired, but I just want to put it this way. We have, when it comes to fundamental rights in the United States of America, always had balances. You have freedom of speech, but you cannot yell fire in a crowded movie theater. Understanding the balances here, and here we have as the honorable **Sheriff Ross Teeple** has said, you know, we have safety concerns, but to me, we have gone way out of balance now when it comes to certain societal interests in public safety and concerns there with violating the average American's sense of fundamental rights to privacy, to speech, to be moving without government surveillance, and so much more. We are way out of balance right now. In fact, we are out of control for any government, state, local, or federal, to easily abuse the fundamental rights that we all assume we have a right to that these cameras seem to be so seriously violating. Correct?

Chad Marlo: Yes, that is correct. Although I would say that just because you are out of balance does not mean that there is a balance to be found. Sometimes things are simply too dangerous to use.

Senator Cory Booker: Understood. Thank you, **Mr. Chairman**.

Chairman Hawley: Thank you, **Senator Cory Booker**. Just let me follow up on that, **Mr. Chad Marlo**, because it seems to be a suggestive line of questioning. When you have this amount of data available, the temptations to use it are going to be absolutely incredible, if not irresistible. And I'm just thinking for those of us who are supporters of the Second Amendment, we've long feared national databases of any kind. You can easily put these cameras up in front of a gun show or near a gun store or a range. You can put them up in front of pregnancy care centers and you can do all the same things that **Senator Cory Booker** was talking about. You can query all the same: show me who's going here, show me who's doing this, show me what time they leave, show me what vendors are supplying these various places, right? And you can create those same patterns using this unbelievable data that basically at this point has no meaningful curbs on it. I mean, isn't that correct?

Chad Marlo: The only thing incorrect about what you said, **Senator Hawley**, was you said *"could."* You should say *"are."* They're doing all those things right now. And again, you know, it reminds me of the movie Field of Dreams. A lot of people say Minority Report, I'm thinking Field of Dreams today. If you build it, they will come. And if you create those temptations, if you create the tools that government need to go after whatever population it is—and I so much appreciate that you're bringing abortion care seekers and gun owners because they are part of the same community when it comes to the threat of mass surveillance—so yes, absolutely, this is something we need to be worried about because when you create the temptation, when you create the option for population control, at some point someone's going to use it.

Senator Cory Booker: Mr. Chairman, can I ask you, I'll make a point to you if possible just as a follow-up, even though you have the same hair issues as our witness. Sure. What's even more frightening than your government, I imagine, is that there's no data security here. And at a time that we're seeing more and more hacks, more and more sophisticated hacks, people using AI to supercharge their ability, the fact that this information could be made available—and you and I both know this because we spent a lot of time in SCIFs—for foreign nationals to hack this and access this information and be able to use it against us, it presents a serious present risk.

Chairman Hawley: And you read my mind. I wanted to ask you, **Mr. Ben Jordan**. The **CEO of Flock** has said, and let me just make sure that I get this right because I think he said this in a letter to a sheriff in Staunton, Virginia. He said in response to a specific query from the sheriff that **Flock** has never been hacked. I think we've got it right here. He says, *"Hi, Virginia Staunton PD team, I'm writing you directly because I want there to be zero confusion about what's happening. Flock has never been hacked. Period. Ever. Period."* Now, based on what you know, is that accurate?

Ben Jordan: I would say that's inaccurate. The company has at various times changed the definitions of the word hacked, tracked, data breached. But in the general definition of accessing unauthorized data, yes, I would say that they've been hacked.

Chairman Hawley: How vulnerable, you've studied this, you are, as you said earlier in your own introduction, a hacker yourself. I mean, how vulnerable, in your professional opinion, are **Flock** systems that contain all of these images? Billions with a B, billions of images. Probably everybody in this room, anybody who's driven a vehicle of any kind, I'm sure we're all on the database. So, how vulnerable are their systems to hacking and then manipulation in the sort of ways that **Senator Cory Booker** was just talking about?

Ben Jordan: In general, one sort of analogy that I really like is if you were in a tiny little box and you wanted to make sure that no ants could get in the box and you were equipped with Raid and a shoe to smash the ants or whatever, you know, you could maybe caulk up the holes. You could pretty much make sure that no ants are going to get in your box and that's great. But if you lived in a **30,000 foot warehouse**, whether ants get in or not is up to the ants, not you. And that's a lot of the way, that's kind of how I look at this in terms of why create this much data when we can't secure it.

But to answer your question a little bit more technically, the **Flock** devices that we tested were running on an old version of **Android** that has been out of service for years. And newer devices of **Flock** run on a modified kernel of **Android**, which is far from government grade security, but it is better than the older ones. But to be fair and to be completely frank, nobody required them to have government grade security. Law enforcement infrastructure has been using **Flock** for 9

years without any form of cyber security regulation or requirements. So expecting a tech startup to adhere to those standards is a little lofty to me.

Chairman Hawley: So are you telling me that they're basically using like 10-year-old **Android** phones as the cameras?

Ben Jordan: Not phones. They're running hardware that was running the **Android operating system** and since then they've had their own build of **Android** that they could secure a little bit better than they had.

Chairman Hawley: A decade old, you said in some cases the technology is a decade old.

Ben Jordan: Yeah. **Android Things 8.1** I believe was the core operating system, which was initially made for stuff like refrigerators and stuff. It's a way where you could run **Android** without a screen essentially. That's why that operating system exists.

Chairman Hawley: So, how easy would it be for a bad actor to download, modify, and/or upload false **ALPR** data into this system? I mean, could that be done?

Ben Jordan: Yeah. So right with those older cameras, the ones that we had tested, I would say that the hardware requires a light to moderate knowledge of **Android debugging**. But I did find an administrative interface, as I mentioned earlier, online of live cameras, which is easy as clicking a link and then hitting a delete button to get rid of footage or something like that.

Chairman Hawley: Well, could you just say that again? As easy as clicking a link and then hitting a delete button.

Ben Jordan: Yeah, I found them on a commercial search engine that searches for things like internet of things devices and we found over 60 cameras that gave—it was the administrative interfaces and it gave us access to 30 days of the past footage of those cameras. And these weren't **ALPRs** in the sense of what we're usually talking about. **Flock** makes a lot of different cameras. They make the **Flock Condor** camera, they make the older Falcon ones which are **ALPRs**, and I think we'll be talking about that a little bit more today because that also kind of defines what AI is, like how it's being used and stuff. But in this case, they were pan-tilt-zoom cameras, so they would actually follow people. And in some cases, I was able to go back a week and read what was on someone's phone screen as they were texting somebody walking under the camera.

Chairman Hawley: You could read what someone had on their phone while they were just walking by the camera.

Ben Jordan: Yes. And I could actually send the link to you and you would have just clicked it and browsed this interface from your phone.

Chairman Hawley: That's extraordinary. I mean that's just extraordinary. Let let me bring this back to the very real personal cost. **Miss Lindsay Isaacs**, I just want to come back to you and your extraordinary story because I think it illustrates the dangers here in this technology if it's not properly cabined and accounted for. I think we have a picture of you with your beautiful new Durango here. Here it is, I think right, this is you and that Durango does look like it's in pristine shape.

Lindsay Isaacs: Yeah, that was the day I got it.

Chairman Hawley: This is the day you got it. All right. You kept it very nice. Now, as I understand it, the Durango that was involved in the vehicular crash that indeed caused three other people to die—it was a vehicular homicide—that Durango was maroon red. Is that correct?

Lindsay Isaacs: Correct.

Chairman Hawley: This Durango doesn't look red to me. What color is this?

Lindsay Isaacs: It's a black Durango.

Chairman Hawley: This is a black Durango. So, here you are returned as a false positive out of an AI search and a **Flock** system. We know it wasn't a traditional license plate search because your car was never there, correct? There were no images of your car at the scene. Is that correct?

Lindsay Isaacs: Correct.

Chairman Hawley: And there was no assertion by anybody ever that you were there. Is that correct?

Lindsay Isaacs: Correct.

Chairman Hawley: It was just that the **Flock** cameras, based on some description, some general description entered into them, the AI pulled out your car and said, *"This is a match."* Correct. And that led to 13 days in jail for you, including solitary confinement, and you very nearly lost your entire livelihood. Isn't that right?

Lindsay Isaacs: I was facing life in prison. It just I can't even believe it to this day.

Chairman Hawley: All because the AI falsely tagged you.

Lindsay Isaacs: Yes.

Chairman Hawley: And that brings me to what may be, I guess, my final point, which is a comment that the **Flock** CEO said recently about the trade-offs that we just have to make in this new technological age. He said that, you know, in this age of **Instagram** and **Facebook**, etc., I

think maybe we have the quote here for you. We've all just agreed to surrender our privacy. He says, *"I think it's important to take a perspective of we've already given up the traditional sense of privacy because we have Instagram and Facebook and the internet and we live in a pretty safe world given those trade-offs."*

I just want to ask everybody in this room, do you want to make that trade-off? I mean, are we going to live in a world where we may all have to suffer the deprivations that **Miss Lindsay Isaacs** did because some robot decides that we were at the scene of a crime, when in fact we were never there at all, and there's just nothing we can do about it? I just suggest to you that this viewpoint is the problem.

I want to end where I started. The Constitution is as valuable and as valid today as it was when it was first written. If anything, the Bill of Rights protections are probably more important today than they were all those years ago because the threats to our liberties are actually much greater, and the technology that both bad foreign actors, private actors, corporations, and government have at their disposal are much more powerful. We need the Bill of Rights more than we ever did, and we've got to find a way to enforce it. I want to thank all of the witnesses for being here. Thank you for your testimonies. Thank you for your work. Thank you, **Senator Cory Booker**. Thanks to our audience. Let me see here, I think I'm supposed to read something about how long the record is going to be open.

The record for this hearing will remain open for one week until Wednesday, September 30th at 5:00 p.m. for the submission of statements and questions for the record. And with that, the hearing is adjourned.

DESCRIPTION:
***Senator Hawley EXPOSES The Network of FLOCK CAMERAS Across The Country* (1:28:23) [Video]. YouTube.**

Surveillance State or Public Safety?
An Analysis of the Flock Safety ALPR Network
https://www.youtube.com/watch?v=KCEdX3o5KfU&t=4886s

Source Material: Senate Judiciary Committee Subcommittee Hearing Transcript

- **Video Title: Senator Hawley EXPOSES The Network of FLOCK CAMERAS Across The Country**
  Channel: Senator Josh Hawley; Video Duration: 1:28:23 minutes
  Publish Date: September 28, 2026
  Official Hearing Record: Senate Judiciary Committee Subcommittee on Crime and Counterterrorism (Hearing held September 23, 2026)

Subcommittee Leadership

- **Senator Josh Hawley**
    - **Title: Chairman** (1:21:50)
    - **Organization: Senate Judiciary Committee Subcommittee on Crime and Counterterrorism** (1:08:10)
    - **Role:** Convened and led the hearing; presented documented evidence, letters, and patent applications exposing **Flock's** AI capabilities, lack of oversight, and safety tracking features (1:08:00).
- **Senator Dick Durbin**
    - **Title: Ranking Member** (1:08:10)
    - **Organization: Senate Judiciary Committee Subcommittee on Crime and Counterterrorism** (1:08:10)
    - **Role:** Co-led the hearing; raised critical bipartisan concerns over mass data harvesting, commercialization of private data, and localized loop-holes used by federal agencies like ICE (27:31).

Witness Panel

- **Lindsay Isaacs**
    - **Title: Victim of ALPR Misidentification** (1:08:38)
    - **Organization:** Private Citizen (Palm Coast, Florida) (1:08:38)
    - **Role:** Testified about being falsely accused of vehicular homicide and imprisoned for 13 days in solitary confinement/maximum security due to an AI false-positive tag generated by a **Flock** camera network (1:08:38).
- **Alistair Whitney**
    - **Title: Legislative Counsel** (23:39)
    - **Organization: Institute for Justice (IJ)** (23:39)
    - **Role:** Represented a nonpartisan public interest law firm litigating warrantless surveillance; testified on how centralized **ALPR** networks allow retroactive, warrantless tracking of citizens across state lines (23:39).
- **Sheriff Ross Teeple**
    - **Title: 25th Elected Sheriff of Pinal County** [0.1.216-0.1.217]
    - **Organization: Pinal County Sheriff's Office** (Arizona) [0.1.216-0.1.217]
    - **Role:** Provided a law enforcement perspective as one of the first leaders nationwide to cancel his agency's **Flock** contract, warning against an AI-driven private surveillance dragnet replacing constitutional rights [0.1.218-0.1.221].
- **Ben Jordan**
    - **Title: Independent Cybersecurity Researcher / Hacker** [0.1.258-0.1.261]
    - **Organization:** Self-Funded / Independent [0.1.258-0.1.261]

  - **Role:** Investigated hardware vulnerabilities; exposed severe flaws including dark web sales of law enforcement accounts, unencrypted streaming feeds, and a physical exploit that allows a device to be hijacked in under a minute [0.1.263-0.1.272].

- **Chad Marlo**
  - **Title: Senior Policy Counsel** (29:49)
  - **Organization: American Civil Liberties Union (ACLU)** (29:49)
  - **Role:** Leads the **ACLU's** *"Get the Flock Out"* national campaign; testified on the emergence of the "surveillance industrial complex" driven by venture capital profits, concluding that **Congress** must completely ban federally funded agencies from using **ALPRs** (26:24).

Other Lawmakers Mentioned or Present

- **Senator Katie Britt** (Subcommittee Member) – Questioned witnesses regarding DOJ oversight and guidelines published by the **National Sheriff's Association** [0.1.233-0.1.236].
- **Senator Alex Padilla** (Subcommittee Member) – Questioned witnesses regarding direct versus indirect data loopholes utilized by federal immigration authorities (**ICE**) [0.1.241-0.1.248].
- **Senator Richard Blumenthal** (Subcommittee Member) – Questioned witnesses regarding state-level protections, preemption, and Connecticut's **Senate Bill 397** surveillance restrictions [0.1.249-0.1.253].
- **Senator Cory Booker** (Subcommittee Member) – Questioned witnesses on data exploitation risks targeting personal liberty, Second Amendment gun owners, and reproductive care seekers (26:01).