

Eyes On You

The Rise of Mass Surveillance in Ohio



ACLU
of Ohio
Report

Published August 26, 2026

ACLU
Ohio

Table of Contents

A Brief Overview of Government Surveillance.....	1
What is an ALPR?.....	1
Let’s Talk Flock (and Other ALPR Vendors).....	2
What are the Stakes?.....	4
Questions You, and Your Community, May Have.....	5
Are ALPRs Constitutional?.....	5
What Regulations Check ALPR Use by Law Enforcement in Ohio?.....	5
What Companies Other Than Flock Should be on My Radar?.....	6
How Much Does Surveillance Cost?.....	6
Are Hotlists Always Accurate?.....	7
Is Surveillance a National, State, or Local Problem?.....	7
Surveillance Can, and Should, Be Rejected.....	8
Statewide Resistance.....	8
Local Efforts.....	9
Resisting Government Surveillance: An Activist’s Checklist.....	10
Learn more about Surveillance in your community.....	10
Build Coalition and Community.....	10
Activist’s Checklist.....	11
Choose your Goal.....	11
Identify opportunities to influence local surveillance decisions.....	12
Publicly Advocate Your Goals.....	12
Practical Resources.....	13
Model Community Control Over Police Surveillance Ordinance.....	13
Model ALPR Legislation.....	13
Tough Questions.....	14
Letters to the Editor and Op-Eds.....	15
Public Records Requests.....	16
Public Records Requests Template for ALPR Contracts.....	17
Public Records Requests Template for Audit Information.....	18
Public Records Requests Template for ALPR Regulation.....	19
Public Records Requests Template for Any and All Surveillance Technology Used.....	20
Other Useful Information.....	21
References.....	21
Appendix.....	23

A Brief Overview of Government Surveillance

Government surveillance is, unfortunately, not new, and has existed in some form or another in this country since at least the 18th century. The earliest surveillance laws on record in the United States were ‘lantern laws’ which required the constant identification of Black, Mixed-Race, and Indigenous people to constantly identify themselves as a “non-white” person. Flash forward nearly 300 years later, and the bulk of the impact of surveillance laws continue to fall on BIPOC communities in the United States. Surveillance technology has taken many forms over the centuries, such as direct spying on citizens, surveillance cameras at street corners, or wiretapping phone lines. In recent decades, the list of surveillance technologies utilized by our government has not just expanded; it’s grown exponentially, fueled by the deep pockets of Big Tech. Drones outfitted with cameras are increasingly employed by law enforcement agencies to respond instantly to 911 calls or to investigate incidents. Biometric technology, including facial recognition software, is now used by [U.S. Customs and Border Protection](#)

at all international airports, processing hundreds of millions of people and their biological characteristics as they enter the U.S.¹ Cell site simulators, also called “Stingrays,” mimic cell towers to intercept and collect data from mobile phones in their vicinity.² And those are just the tip of the iceberg. Recent reports are wary of defense contractor Leonardo [US’s new surveillance system](#), ELSAG SignalTrace, which can add Bluetooth, Wi-fi, and radio frequency identification devices (RFID) data collection capabilities to standard license plate readers.³ This will give law enforcement the ability to harvest identifying information from every consumer device in range including your smartphone, earbuds, even pet microchips, all without a warrant.

Legislation at the federal, state, and local level is failing to account for the proliferation of mass government surveillance, especially with the pervasive spread of these ever developing and evolving technologies. This also includes the rapid spread of automatic license plate readers (ALPRs) powered by artificial intelligence and utilized by law enforcement and local governments.

Biometric technology is the measurement and analysis of biological data like fingerprints, retinas, irises, voice patterns, facial patterns, and hand measurements. Facial Recognition is a type of biometric technology that is designed to identify or verify an individual by analyzing their unique, measurable facial features.

What is an ALPR?

An automatic license plate reader is a mobile or fixed-location camera used to take photographs of license plates, digitize them, and then store, process, and search captured data in real time or over the course of months or even years.⁴ Law enforcement claims these cameras help them solve and prevent crimes, but they also track law-abiding citizens in the process. ALPRs are not new; the technology was developed in the 1970s and was first used in the U.S. in 1998 by the U.S. Border Patrol.⁵

ALPRs are small and unassuming - if you use public roads throughout Ohio, you’ve probably driven by them hundreds of times without even noticing.

Traditionally, ALPRs have access to “hotlists”—databases with license plates flagged as part of a criminal investigation, such as having a warrant out for the owners arrest, being tied to a missing person, or similar criteria stored in the Federal Bureau of Investigation’s National Crime Information Center (NCIC). Newer, AI powered ALPRs are unique in that they no longer just document your license plate, identifying features like the color, make, model, bumper stickers, roof racks, and visible damage of every car that drives by. These identifying features then are stored and searchable in the vendor’s

system. The data collected by ALPRs is often retained by police departments for considerable periods of time. While a few states and cities regulate how long agencies or companies can keep the data collected by ALPRs, most don’t. This opens the door for wildly different approaches across jurisdictions for handling that data, and how long it can be accessed. This allows the government to track where people travel in their cars, including what doctors they go to, what political or religious meetings they attend, where they shop (including a gun store or show), and even where they sleep at night.

Let's Talk Flock (and Other ALPR Vendors)

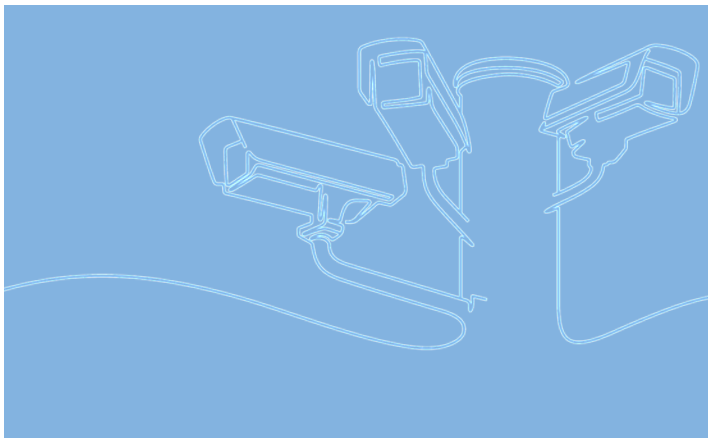
Flock Safety is a \$7.5 billion dollar company founded in 2017 that produces AI enabled ALPRs - which they boast capture “billions of monthly plate reads.”⁶ Flock’s marketing is built on the impossible promise that their technology will help local law enforcement solve “[every single crime that happens in America](#).”⁷

In addition to ALPRs, Flock sells video cameras, gunshot/audio detection devices, drones, and various software for law enforcement.⁸ Flock claims that facial recognition technology is not used in any of their products, but many of their cameras come equipped with a “Freeform AI” feature which allows you to search and track people captured based on behavior, gender, and identifiers like clothing in plain terms like “man in black cowboy hat” or “woman in blue dress.”

What’s most shocking about Flock’s products is the sheer volume in use. Flock reports their ALPRs are “trusted” by 1,000+ businesses, 5,000+ law enforcement agencies, and 6,000+ communities across the country. Various estimates, including from the website [DeFlock.me](#), indicate there are over **100,000 ALPRs** nationwide, with the vast majority of those produced by Flock.⁹

To put it bluntly, Flock has been a key force in the construction of a nationwide mass surveillance network in less than a decade since its founding.

That network is important to understand. Those 100,000 cameras are not just collecting data in isolation. All Flock ALPRs are connected by a default nationwide data sharing feature, which allows any Flock customer to search other customers’ data. Flock does allow this setting to be toggled off. The company also provides what it calls a transparency portal, where a law enforcement agency or city can enable a publicly accessible website hub that documents the number of plate reads, hot list hits, number of searches, and lists all third-party entities who have had access to their camera’s data.¹⁰ However, out of over 5,000 law enforcement agencies that Flock claims use their ALPRs, only about 700 have enabled this transparency feature, and it is unknown exactly how many allow or limit data sharing, or to what extent.¹¹



Gunshot and audio detection devices listen 24/7 for loud noises to identify gunfire and alert law enforcement. Some praise these systems for cutting down response times, but many contracts have been canceled after low confirmations of shootings, high cost, and underwhelming effects on gun violence. ShotSpotter is a popular vendor, but Flock Safety has also introduced its own system, Raven. It reports not only gunshots, but sounds it recognizes as vehicle collisions, street takeovers, and “other disruptive community events” raising concerns about the government listening in on people’s day to day activities.



Let's Talk Flock (and Other ALPR Vendors) *continued*

Flock also claims to refrain from contracting or sharing data with federal agencies like Immigration and Customs Enforcement (ICE). However, a pilot program was uncovered that gave ICE and other federal agencies explicit access to Flock data for a window of time in 2025.¹² Customers are also free to share data with federal third parties as they wish.¹³ Furthermore, the longer the data is retained, the easier it is for the system to develop what Flock calls a “Vehicle signature” which are detailed assessments on cars and driver behavior. All of this can be done with or without license plates with AI detection, giving law enforcement the ability to unjustly profile people based on an algorithm’s assessment of their behavior.

Flock also claims that it does not own customer data, but per the [standard contract](#), “Customer hereby grants to Flock a limited, non-exclusive, royalty-free, irrevocable, perpetual, worldwide license to (a) use and disclose Customer Data to provide the Flock Services; and (b) use Customer Data to support and improve Flock’s products and services,” giving Flock the ability to share data without customer permission “if legally required

to do so or if Flock has a good faith belief that such access, use, preservation or disclosure is reasonably necessary to comply with a legal process, enforce the agreement between Flock and the customer, or detect, prevent or otherwise address security, privacy, fraud or technical issues.”¹⁴

ACLU of Ohio translation: This catchall language gives Flock unlimited control over any data they choose, collected by their cameras. Law enforcement and government officials signing these documents are essentially giving a private company a pass to share our data nationally, or even globally if they deem it appropriate.

Note: Flock is not the only ALPR company on the block—far from it. A subsequent section of the toolkit covers these competitors in greater detail.



Our government is using Flock and other products to create a vast network of connected tracking devices that follow you from coast to coast, dissect your behavior, document your traits, and then save that data so that anyone with access – potentially thousands of miles away—can spy on you, too.



What are the Stakes?

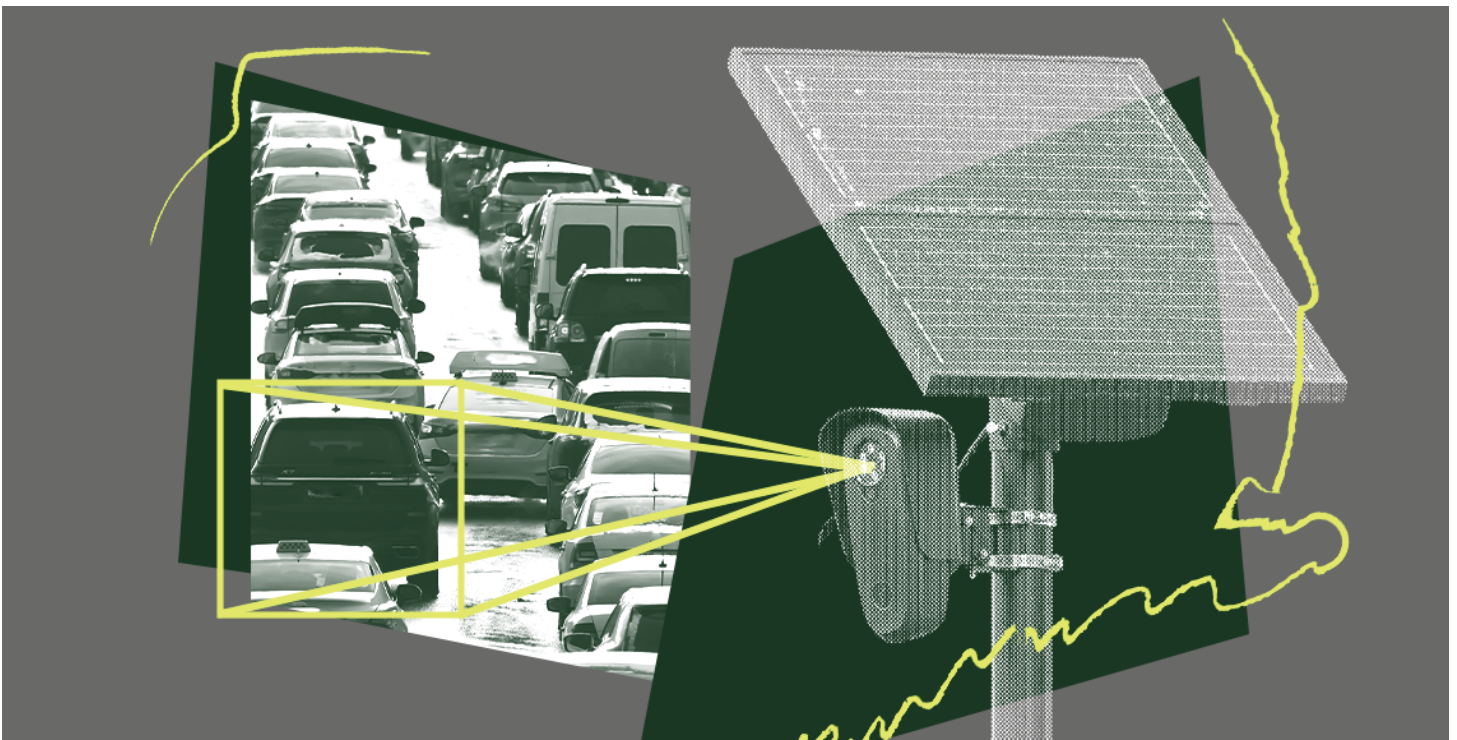
...and why do we care

Government use of these technologies at this scale, with these capabilities, and consequences is dragnet surveillance. **Dragnet surveillance is the broad, systematic surveillance of all people in a given area with the meek justification that it is used to identify potential criminal activity.** Potential is the key word there. Law enforcement and governments are collecting data on millions of Americans everyday with no warrant, no probable cause, and no individualized suspicion of wrongdoing because it *might* help solve a crime. The depth of information and the ability to build a profile of an individual with identifiers such as political party affiliation, sexual orientation, gender identity, religion, and daily routine make the lack of regulation and continued use of technology like ALPRs an invasive, intolerable violation of civil liberties.

The use of surveillance technology has always invited its abuse. The NYPD used ALPR devices and other [surveillance tactics](#) to abusively surveil mosques and Muslims in the 2000s.¹⁵ In recent years, ICE has been accessing ALPRs, in some cases illegally, for searches related to immigration and capitalizing off facial recognition and biometric technology like Mobile Fortify.¹⁶ Both are utilized to create probable cause to detain and arrest suspected non-citizens without a warrant. Facial recognition is known to be inaccurate, having resulted in [several arrests](#) of innocent people for crimes they did not commit.¹⁷

A Texas Sheriff used [Flock cameras](#) to search for a woman who self-administered an abortion, under the guise it was a “missing persons case” when it was in fact a criminal investigation.¹⁸ Multiple officers, including one in [Sedgewick, Kansas](#), have used ALPRs to track and stalk ex-lovers, and even their new partners.¹⁹ The cameras have even resulted in wrongful arrests, such as when [a Colorado police department](#) arrested an innocent woman for a package theft.²⁰ These are just a few of the hundreds of examples of misuse that have been documented with police use of ALPRs and surveillance technology, not to mention those that go unreported every day.

As Ohioans, we value the liberty and freedom to live as we choose, without the fear of government surveillance. Think about when you know you are being watched. What it’s like to have a cop behind you on the road, a proctor watch you take a test, or a referee watch you compete. You probably feel nervous, scrutinized, and maybe even a little afraid – even if you are not doing anything wrong. Cameras like ALPRs have a similar chilling effect, as the constant awareness of being watched deters people from participating in civic and democratic life. You might then think twice about attending a protest, going to your place of worship, or just moving through your daily routine, for fear it will later be used against you.



Questions You, and Your Community, May Have



Are ALPRs Constitutional?

As far as the U.S. Supreme Court is concerned, it is an open question as they have not yet accepted a case addressing the constitutionality of mass surveillance specifically using automatic license plate readers. However, **there are some encouraging signs due to the Supreme Court's rulings on a series of three cases related to government surveillance and modern technology. :**

U.S. v. Jones (2012)

The Fourth Amendment requires law enforcement to first obtain a warrant before attaching a GPS device to a criminal suspect's car to track their travels and movements.²¹

Carpenter v. U.S. (2018)

When law enforcement obtains a person's cell phone location information, revealing their past travels, it is a "search" for Fourth Amendment purposes and a warrant is required for legal access to those records.²²

Chatrue v. U.S. (2026)

Much like Carpenter, when law enforcement utilizes a "geofence warrant" to get cell phone location information from everyone in a defined area, and uses that data to narrow a list of suspects, it is a "search" requiring a warrant.²³

Throughout these (so far) three cases, the U.S. Supreme Court finally acknowledged the capabilities and uses of modern surveillance technology and how past Fourth Amendment court decisions about such things as legal "expectations of privacy" do, or do not, apply in current times.

That is, the judicial bedrocks of Fourth Amendment law were established well before these invasive, highly revealing tools and technologies were invented, or even anticipated. In the same way the First Amendment had to account for television, movies, the internet, and other things not in existence when the Bill of Rights was adopted, Fourth Amendment protections must now be considered in light of our growing surveillance state and the technology fueling it.

Given all this, it is hard to believe automatic license plate readers will not be one of the next specific devices to be considered by the U.S. Supreme Court. The good news is, noting the same logic and constitutional concerns present throughout all three cases mentioned above, we have reason to be hopeful ALPRs will be the next mass surveillance domino to fall.



What Regulations Check ALPR Use by Law Enforcement in Ohio?

There is no overarching state or federal law that regulates the use of ALPR technology by law enforcement, so the rules are determined either by the city or county in question, or often by the law enforcement agency themselves. This means vastly different training for people with access to data, differing lengths of data retention, and vastly different data sharing regulations. **The only sort of guideline present in Ohio law is that the footage and data output by ALPRs are not considered public records. So citizens, in theory, should not have access to footage or information.** In multiple cases, though, ALPR data has been leaked, leaving personal data potentially in the wrong hands.²⁴ Failing to implement other guardrails on this kind of invasive technology leaves the door open for — at worst — illegal privacy violations, and — at best — a hodge podge of drastically different and confusing guidelines.



What Companies Other Than Flock Should be on My Radar?

The name “Flock” has become somewhat synonymous with surveillance in recent media coverage, but many other companies are making similar products that threaten our privacy. Motorola Solutions, Axon, Sound Thinking, and Genetec are just a few other companies who are also producing ALPRs and other surveillance equipment for government use. [Motorola Solutions](#), previously Vigilant Solutions, has a history of selling data to third parties such as ICE, data fusion centers, and repossession companies.²⁵ Many Ohio cities, like Columbus and Cleveland, use a mix of different companies’ technology, with hundreds of Flock cameras in operation as well as a Columbus Police Department contract with Axon for body cameras, drones, and ALPRs mounted to patrol cars.²⁶ Columbus and Cleveland also utilize Sound Thinking’s ShotSpotter gunshot detection.



How Much Does Surveillance Cost?

Figuratively, the cost of repeatedly violating our privacy rights is limitless. Literally, surveillance technology costs taxpayers thousands, or even millions of dollars to install and maintain in their localities. For example, Cleveland’s new six-month contract with Flock is set to cost residents [\\$125,000](#) dollars for 100 cameras.²⁷ This is after Cleveland Mayor Bibb pushed through an [\\$835,000](#) contract renewal with ShotSpotter without city council’s approval.²⁸ [Columbus](#), as discussed above, also uses a variety of different surveillance systems, including but not limited to police department Flock contracts, like Ohio State University Police Division’s \$652,050 contract, CPD’s \$26 million dollar contract with Axon, and \$6.5 million spent on ShotSpotter. **Prices seem to vary, even with products from the same company, but the bottom line is that surveillance is an expensive cost to your community.** Below is data reported by WOSU media that details the staggering spending of many Central Ohio law enforcement agencies on Flock ALPRs alone.²⁹

Police Department	Number of Cameras	Contract Total
Bexley Police Department	10	\$70,800. ⁰⁰
Blendon Township Police Department	8*	Unknown
Clinton Township Police Department	7*	Unknown
Columbus Airport Police Department	19*	Unknown
Columbus Division of Police	38	\$228,000. ⁰⁰
Dublin Police Department	25	\$135,700. ⁰⁰
Franklin County Sheriff’s Department (Prairie Twp.)	14**	Unknown
Gahanna Police Department	21	\$139,000. ⁰⁰
Grandview Heights Division of Police	8	\$100,000. ⁰⁰
Grove City Division of Police	32	\$199,800. ⁰⁰
Groveport Police Department	20	\$31,450. ⁰⁰
Hilliard Division of Police	4	\$24,500. ⁰⁰
Madison Township Police Department	5	\$78,500. ⁰⁰
Minerva Park Police Department	4	Unknown
New Albany Police Department	8	\$24,000. ⁰⁰
Ohio State University Police Division	63	\$652,050. ⁰⁰
Perry Township Police Department	0****	
Upper Arlington Police Department	20	\$91,500. ^{00***}
Westerville Police Department	16	\$70,650. ⁰⁰
Whitehall Police Department	30*	Unknown
Worthington Division of Police	14	\$43,100. ⁰⁰

* Did not respond to Freedom Of Information Act request, numbers obtained through media reports, transparency portals, or publicly published FOIA. **Franklin County Sherriff’s Office does not have any contract with Flock, but Prairie Township, which does not have its own police, provides Flock access to FCSO. ***Price obtained when number of cameras for Upper Arlington was only 6, may have changed as cameras increased in number **** Has a contract with Flock, but no cameras were discovered in WOSU’s investigation



Are Hotlists Always Accurate?

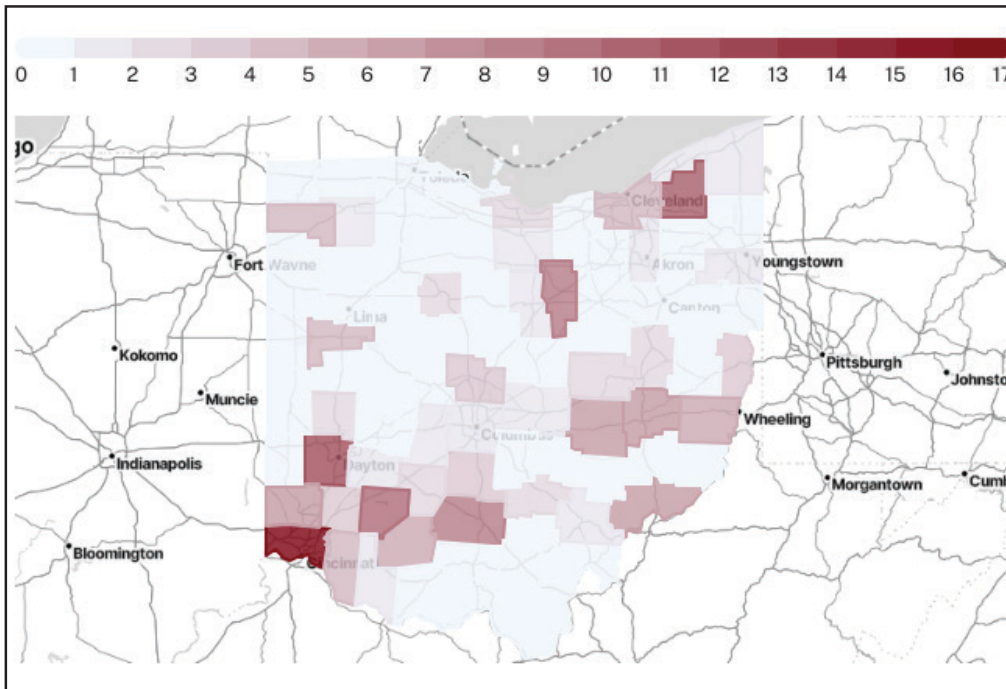
Flock and other ALPR vendors rely heavily on license plate “hotlists” that contain plates of cars suspected stolen, related to missing persons, or that belong to people with warrants issued against them. Those lists, if not regularly updated and edited, have been known to contain inaccurate information that could lead to wrongful arrest. Flock uses the Federal Bureau of Investigation’s (FBI) NCIC database, which is notoriously inaccurate, leading to harmful consequences for those incorrectly identified. Federal law requires that government agencies maintain records used to make “any determination about any individual” with “such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.”³⁰ That doesn’t seem like too much to ask but when it comes to its NCIC database, the FBI has exempted itself from that law meaning the NCIC often suffers for it.³¹



Is Surveillance a National, State, or Local Problem?

Trick question. *It is a national, state, AND local problem.* Even if local surveillance is addressed, you are still being watched throughout your state if you decide to travel, whether that be by drones, cameras, biometrics, SignalTrace devices, audio detection, or of course ALPRs. Even cameras outside of Ohio can affect Ohio residents, with ALPRs along interstates or in towns passed and visited by Ohioans capturing our data in addition to cameras in our communities.³² ALPRs are also being considered for use by the federal government. The FBI is looking for a vendor, such as Flock or Motorola, to complete a [\\$36 million dollar contract](#) that would attempt to monitor major highways and large percentages of roads and communities of the six regions the FBI is interested in monitoring.³³ The more aware the public is about the privacy and safety concerns of surveillance technologies and how they are used in Ohio, the better we can all tackle the issue on a national scale.

Ohio Counties with Right of Way Agreements signed with ODOT in 2025



A recent ACLU of Ohio public records request to the Ohio Department of Transportation (ODOT) revealed that in 2025 alone, the department signed 157 agreements with 60 unique law enforcement agencies to install ALPRs at rights-of-way managed by the state.

Surveillance Can, and Should, Be Rejected

Statewide Resistance

While Ohio has little to celebrate in terms of surveillance protections, many states around the nation are setting strong examples of [ways to better protect our privacy](#) through state laws. States have passed laws restricting what ALPRs can see and record, the use of AI detection features, law enforcement parameters, transparency, the use of warrants before launching surveillance drones and more.³⁴ Notably, Illinois passed the [Biometric Information Privacy Act](#), which protects personal identifiers like fingerprints and facial data.³⁵

Other states protect their citizens' privacy by restricting the data retention period for ALPR data, lessening the threat of stored data being used to unjustly profile people without a warrant. Below is a list of the states with a version of those laws on the books, and the varying retention periods allowed. In our opinion, the shorter the period the better, with the best law on the books being New Hampshire's 2007 law restricting data retention for ALPRs to just 3 minutes unless the license plate triggers a hit in the system.³⁶



Year Adopted	State	ALPR-specific statewide data retention period
2026	Connecticut	21 days
2026	Oregon	30 days
2026	Kentucky	90 days
2026	Washington	21 days
2025	Virginia	21 days
2024	Vermont	Near total ban (0 days)
2018	Georgia	30 months
2017	Montana	90 days
2015	Minnesota	60 days
2015	North Carolina	90 days
2014	Tennessee	90 days
2013	Arkansas	150 days
2011	California	60 days
2009	Maine	21 days
2007	New Hampshire	3 minutes

Surveillance Can, and Should, be Rejected *continued*

Local Efforts

Ohioans are fighting back against invasive government surveillance. Groups have formed, such as [Flock No in Cleveland](#), that advocate for the prohibition of ALPRs and similar surveillance technology.³⁷ Yellow Springs and Dayton are the first Ohio cities to adopt ordinances requiring public input on surveillance technology known as Community Control Over Police Surveillance (CCOPS), a proactive measure the ACLU of Ohio champions.³⁸

[Dayton](#) became center stage for the fight against warrantless surveillance in Ohio after concerns that ICE was using Flock data for immigration enforcement. In May 2026, the city of Dayton suspended use of its cameras after they found more than 7,000 cases of searches related to immigration made by outside entities. City officials called the searches an egregious violation of policy, since regulations prohibit the sharing of the data collected by ALPRs to be used for immigration enforcement. Dayton's contract in 2024 had approved \$825,750 on spending on just 35 cameras and the city had received another \$90,000 in grant money for 27 more devices in 2026.³⁹

Dayton literally trashed their contract with Flock, covering the cameras with black trash bags until they can be removed amid citizens' concerns that the cameras were potentially still recording.

While Ohioans are beginning to mobilize against government surveillance, there are plenty of success stories to look to, where communities across the nation have realized they were being watched and did something about it.

According to ACLU National, since January 2025 more than 80 cities across the U.S., from California, to New York, Texas, to Missouri, North Carolina to Wisconsin and beyond, are saying NO to Flock — and this list is only growing.



Resisting Government Surveillance:

An Activist's Checklist

It's time to fight back against government spying. Here is a checklist of steps to make a difference in your community, and advocate for your community's privacy rights..

✓ Learn more about Surveillance in your community

The best way to start tackling surveillance in your community is to understand it. You can look for signs of surveillance technology usage, contracts, or future plans by doing the following:

- Monitor local government and law enforcement agencies' websites and agendas for reference to surveillance, ALPRs, Flock, other companies, or surveillance devices of interest.
- Look for references in local government documents to grants like State Homeland Security Grant Program (HSGP), Urban Area Security Initiative (UASI), and Operation Stone Garden (OPSG) that might indicate funding from DHS for surveillance programs.
- Closely search for and read local news for stories or opinions on surveillance in the area.
- Reach out to your local, state, and federal elected officials, and ask what their stance is on the use of surveillance technology.
- Send a public records request to agencies you suspect are using ALPRs or other surveillance technology (see Public Records Requests under Resources).
- Search [DeFlock.me](https://deflock.me) for evidence of ALPRs in your community.
- Check the crowdsourced map at [ALPR.watch](https://alpr.watch) which includes local government meetings where ALPR cameras will be on the agenda.

Even if you do not initially find evidence of surveillance technology, that does not mean it will never become a problem. You can take preemptive steps to combat surveillance in your community by pursuing a Community Control Over Police Surveillance ordinance (see CCOPS model language under Resources). Continue to keep an eye on the state of surveillance in your area.

✓ Build Coalition and Community

Educating yourself and others is a great first step to combating dragnet surveillance in your community. Once you have a grasp on the state of surveillance in your area, begin reaching out to others in your community to build grassroots momentum. Working within a coalition is an opportunity to create political power, identify allies, and build the narrative for policymakers and the public about why an issue really matters. Some good places to start are:

Putting feelers out to your community

- Seek to meet one on one with individuals in your community also interested in surveillance, whether it be ALPRs, drones, or dragnet surveillance in general.
- Interact with established groups on social media, and/or post your own thoughts to generate interest and potential community support and connections.
- Establish a short list of concerned parties and reach out to determine if they would be interested in collaborating, or if they would aid action against government surveillance in any way.

Meet with the partners, build connection, and begin identifying potential actions you may wish to take.

Any successful organizing group has structure. Designating leadership, support roles, responsibilities, and basic agendas are all necessary steps to building group consensus and leading to grassroots coalition power.

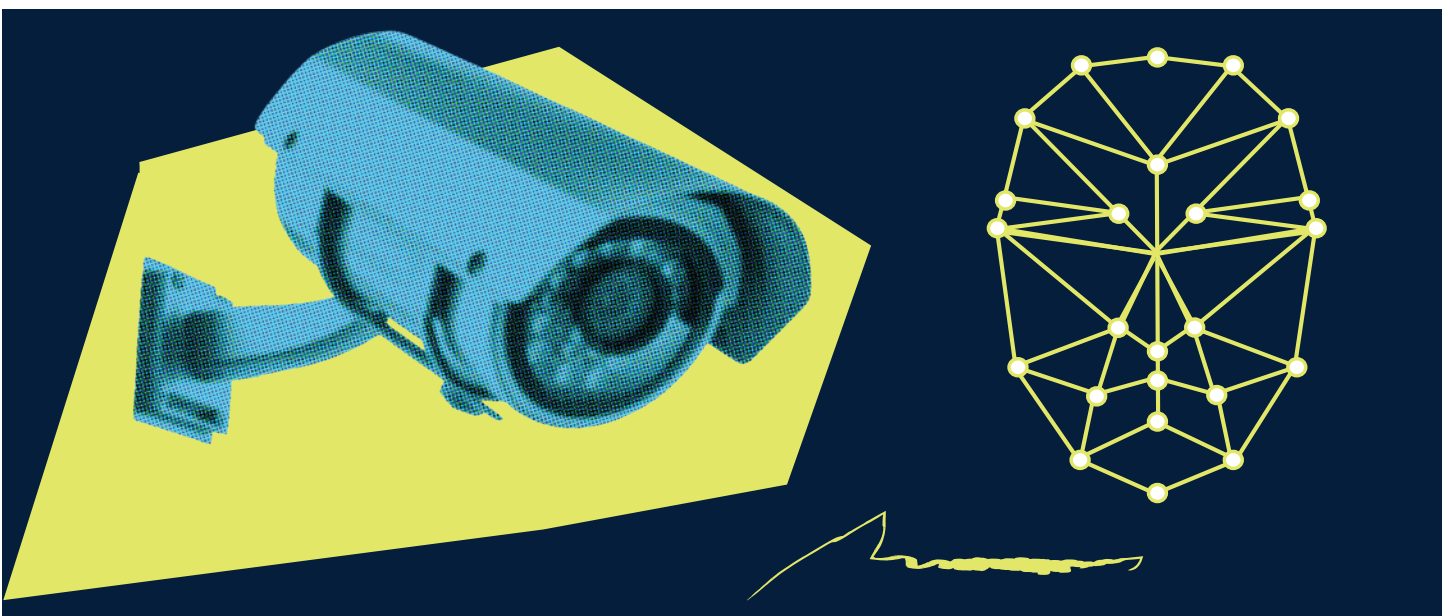
Decide whether regular coalition meetings (on the phone or in person) make sense and set a schedule. After you've started meeting, it is time to develop a course of action.

✓ Choose your Goal

Whether you now have a coalition for change or are striking it out alone, clear messaging and goals are key to success. Government surveillance takes many forms and shapes, so your goals might not look exactly like other groups across Ohio or even neighboring communities. **Important reminder: critically assess the political climate of your community to determine realistic, achievable goals. You might wholeheartedly believe (as the ACLU of Ohio does) that the best option is total elimination of technologies like ALPRs or drones, but if you lack sufficient support from elected officials and fellow residents, you might have to adjust course.** So, keeping that in mind, here are a few avenues your group could take:

- Educate your neighbors on surveillance technology and its use in your community.
- Demand that your community not contract with any vendors of mass surveillance technology.
- When that is not possible, advocate for better contracts that include robust privacy protections and vet the language with the entities entering the agreements, such as a sheriff or city council.
- Push for better regulations for law enforcement using surveillance technology such as:
 - Imposing limits on length of data retention for technologies such as ALPRs.
 - Ensuring all people allowed access to data undergo proper training.
 - Prohibiting data sharing with other departments, agencies, cities, and states.
 - Requiring the use of interfaces like Flock's transparency portal and/or mandating reporting on the use of any and all surveillance equipment and audits of that use with public access.
- Seek the implementation of an ordinance or other legislation that will require public input on surveillance decisions and use in your community, like a CCOPS ordinance.
- Oppose future or current surveillance proposals that are under consideration.
- Advocate for and build a police or surveillance oversight commission of citizens that can monitor the use and performance of surveillance technology.

Once you have strategically identified your goals and policy positions, develop the messaging and narrative you want to present to your community.



Activist's Checklist *continued*



Identify opportunities to influence local surveillance decisions

To achieve your newfound goals, you must find opportunities to make yourself and/or your group part of the conversations. Remember, take every opportunity to stay informed about the current state of surveillance in your area! Some places to start:

- City council and county commission meetings/hearings
- Board of supervisors meetings
- Local police departments forums
- Town halls or forums

Decision makers look different in every community, but you should be reaching out and searching for the individuals responsible for 1) signing contracts with surveillance vendors, 2) implementing regulations on law enforcement, 3) voting on and producing local legislation, or otherwise having influence over your community's privacy and security.

Meeting with decision makers can be intimidating. To ensure a smooth discussion, bring a concrete plan or meeting agenda to articulate and defend your position. Remember to keep calm and compromise when needed, but do not undercut your voice and your power. Our elected officials are meant to serve the public, not their personal interests or a private corporation's bottom line.



Publicly Advocate Your Goals

You've shaped your message, contacted established community leaders, and built a network of like-minded neighbors. It is time to make your fight public and organize action and events in your community. Continue posting on social media and meeting with decision makers, but try and level up and bring your fight against surveillance to the spotlight by:

- Host or sponsor town halls and forums to educate your community about government surveillance and your area's use of it.
- Reach out to local news and pitch your advocacy as a compelling media story. Submit letters to the editor, opinion pieces, or invite the media to relevant events to further spotlight the issue.
- Pack council meetings with allies and line up community testimony to show broad support on the issue.

Remember, success is not always linear. These are some examples of directions to take in your fight to protect local privacy, but you will surely encounter some opposition and setbacks in your journey. Persistence and patience are key in taking on something as daunting as government surveillance. Hopefully, the information, guidelines, and checklists in this toolkit will enable you to fight local surveillance, and empower you to push through when that fight gets difficult.

Conclusion

Given the omnipresence of mass surveillance technology in everyday life, fighting back can feel incredibly daunting. Be that as it may, there always will be real power in advocates and organizers coming together to demand better of our elected officials. It is our hope that this toolkit is one resource you can use in this fight. Protecting and promoting public safety is possible without giving in to mass surveillance. **Together, we can protect our privacy rights AND keep our communities safe.**

Practical Resources

✓ Model Community Control Over Police Surveillance Ordinance

[Community Control Over Police Surveillance](#) (CCOPS) is a campaign that was launched on September 21, 2016, by the ACLU and other advocates in response to growing concerns about surveillance.⁴⁰ Nearly a decade later, unprecedented growth of ALPRs and other invasive technology has made this campaign more relevant than ever. Flock and other surveillance companies have taken the backdoor into our lives, usually without warning or knowledge from the community. The principal objective is to ensure that local residents, through their local elected officials and other government offices, are empowered to decide if and how surveillance technologies are used. To date, 26 jurisdictions have adopted CCOPS across the US, including Dayton and Yellow Springs in Ohio. It is important to remember though that while the ACLU of Ohio supports CCOPS legislation, CCOPS ordinances do not require firm regulations on surveillance technology, it simply requires public input on the matter. You can access the ACLU model CCOPS bill here: assets.aclu.org/live/uploads/2023/08/ACLU-CCOPS-Model-Bill-April-2024.pdf

✓ Model ALPR Legislation

Limit Use of ALPRs

If your goal is to restrict the use of ALPRs in your community but not institute a total ban, this model bill produced by the ACLU may be helpful in your advocacy. The model bill includes clauses that regulate use, data sharing, and data retention, among other important considerations with ALPR technology.

Model Local Automatic License Plate Reader Privacy Bill:

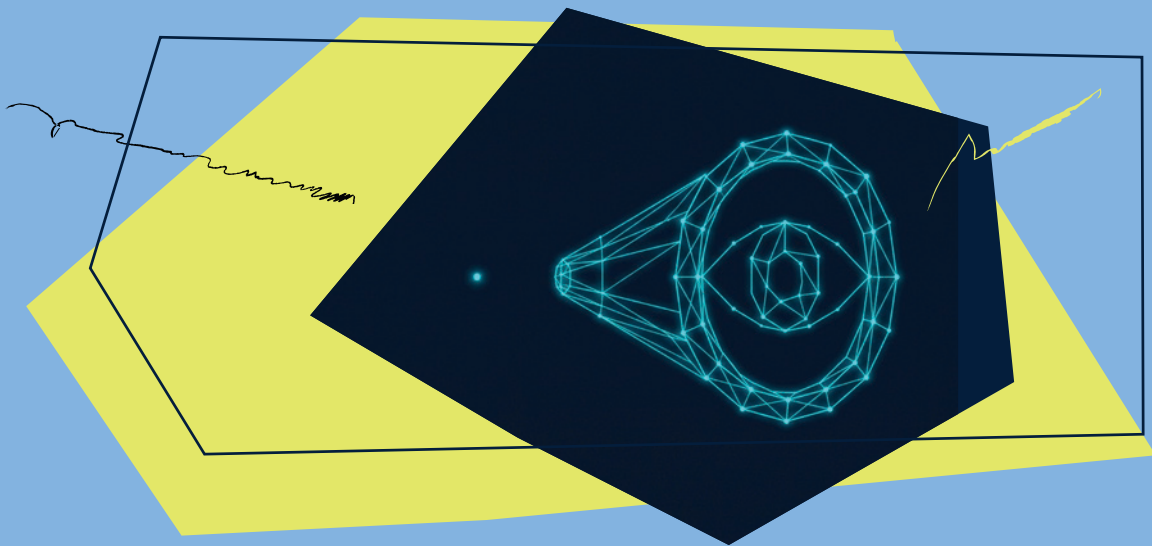
<https://www.aclu.org/documents/local-automatic-license-plate-reader-privacy-model-bill>

Oust Flock

If your goal is to cancel and/ or completely cut FLOCK out of your community, this model bill produced by the ACLU may be the right fit.

Model Resolution for Local Flock Contract Cancellation:

<https://www.aclu.org/documents/model-resolution-for-local-flock-contract-cancellation>



Tough Questions

You may encounter difficult conversations and questions as you navigate your advocacy journey. Below are some examples to familiarize yourself so you can be prepared for potential opposition:

? “Why would I care about government surveillance if I’m not doing anything wrong?”

Even if you do not feel that anything you have or will do is “wrong,” what is considered “wrong” can, and has, changed through different political administrations or cultural shifts. Simply speaking, who is defining what “wrong” is (the government), can be the issue. So, unless you can always trust your government to not have reason to track you based on your party affiliation, race, religion, occupation, or any other identifying factor, you should not want your neighbors to be tracked either.

You are also being surveilled by this technology whether or not you are being specifically searched for suspected wrongdoing; the government can create a log your movements, behavior, and activity with a click of a button. This violates a core principle of our society: that the government should not invade a person’s privacy and collect information just in case they do something wrong. All Ohioans are considered innocent until proven guilty under the U.S. Constitution and should be treated as such.

? “Is being anti-government surveillance a right or left issue?”

Government surveillance may be felt by everyone differently, but it certainly effects everyone in Ohio and the United States regardless of their political affiliation or ideology. The ACLU of Ohio is nonpartisan and sees this issue as a core violation of Ohioans’ civil liberties. A constitutional violation is not a red or blue issue, it’s an attack on everyone in this country’s rights, and in this case, privacy.

? “What’s the big deal about being watched in public?”

Tracking people’s movements is a significant invasion of privacy that can reveal many things about our lives, such as whether a person sees a psychiatrist, attends AA meetings, goes to religious or political meetings, visits gun shops, or even is having an affair. So, while ALPRs and other cameras cannot see behind closed doors, they capture information for governments that were previously unimaginable, invading our expectations and right to privacy in our lives and activities. Furthermore, the more advanced surveillance technology becomes, the more invasive that surveillance becomes. Audio detection equipment hears you, RFID technology detects, and technology like SignalTrace scans and logs regardless of whether you are out in the open or behind closed doors.

? “Doesn’t government surveillance keep us safe?”

Surveillance can help solve some crimes after the fact, but at the exorbitant cost of subjecting people to constant government spying. Many people are unaware of invasive surveillance tactics employed by law enforcement. That lack of knowledge may keep lawful citizens from experiencing that fear and chilling effect, but it also means that would-be criminals are in no way deterred from committing those crimes. Besides, if something only works after the fact, does it really keep us safe?

Your local ALPR data could also be used to enforce anti-abortion, anti-immigrant laws, or other laws not applicable to you or to your neighbors from other jurisdictions. There is even the potential threat that it could be used to assist foreign, authoritarian regimes in some way, such as hunting down political opponents and refugees living in America, since Flock’s default provision gives the company a “worldwide license” to its customers’ data.

It is also important to remember companies like Flock are private entities that the government permits to be the facilitator of data collection on millions of Americans every day. The government and law enforcement already have ample opportunities and reasons to abuse the data collected by ALPRs and other surveillance equipment, and to have such data flowing through a private company creates an additional set of incentives for abuse.

Letters to the Editor and Op-Eds

Letters To the Editor (LTEs) and Op-Eds are powerful tools to influence public opinion, respond to news in your community, and gain support on issues important to you.

A Letter to the Editor (LTE) is a short, direct response to a specific news or opinion article published by the same publication. The letter should be timely, concise, and under 200 words.

An Op-Ed is a longer, standalone opinion piece that allows you to explore an issue in depth, in this case a surveillance issue that you are passionate about. Op-eds require a strong perspective on a relevant topic and are typically around 500-800 words.

What does a basic LTE outline look like?

- **Opening:** Immediately reference the article you're responding to and state your main point. Express your concern or appreciation. This is where you tie your issue to the article in question, take a stance, or correct any errors or misrepresentations. Explain your key point within the first sentence or two to keep the reader engaged.
- **Middle:** Briefly explain your connection to the issue and why readers should care. Use a key statistic, highlight the real-world impact, or share a personal story. End here with a clear call to action.
- **Closing :** In one or two sentences, recap your point and reiterate action items for readers, including where they can find more information on how to get involved.

What does a basic Op-Ed outline look like?

- **Introduction:** Grab the reader's attention with something compelling like a personal story, a surprising statistic, or a connection to a timely event.
- **Your Argument:** Introduce your main argument and explain the problem. This is where you tell the audience why they should care.
- **Build Your Case:** Build your argument in a couple of paragraphs with 2-3 supporting points, using evidence like data, expert quotes, or real-life examples.
- **Closing:** End with a strong, memorable call to action that echoes your introduction.
- **Title:** Finally, review your piece and write a clear, catchy title that reflects your argument.

For LTEs, since you are responding to another piece, you want to submit your response within 1-2 days of the original article. You can email your submission to a publication through their general contact information or upload it to a specific online portal email address or they may have a dedicated email address or webform. It is best to focus on small, local media outlets for the best chances of getting your work published and seen by your community. If you get rejected, try your luck with other local papers and media outlets. For a more detailed look at the process, refer to the ACLU's Guide to Writing Letters to the Editor and Op-Eds [Guide to Writing Letters to the Editor and Op-Eds | American Civil Liberties Union](#)

Public Records Requests

In Ohio, we have the Ohio Public Records Act and Ohio Open Meetings Act, also known as Ohio's Sunshine Laws, requiring government transparency at the state and local level. Public records requests (PRRs) let us peek behind the curtain and gather information to do our own investigations into how decisions are made and how agencies operate.

Unfortunately, it's not uncommon for people, the press, or groups to [hit a wall trying to obtain public records](#).⁴¹ Public offices must provide you with an explanation if your request is denied or if any portion of the record is redacted, and they must explain why the redaction was necessary by citing the legal authority for doing so. If you feel that your request was wrongfully denied, you have two options: 1) file a complaint with the Ohio Court of Claims, or 2) file a writ of mandamus in common pleas court, court of appeals, or the Ohio Supreme Court. There are pros and cons with either choice. If you decide to go this route, you can only pursue one option in accordance with [Ohio's public record law](#).

[In the ACLU of Ohio's Keep An Eye On Your Government-The Activists How To Guide](#), we dive into more depth on Ohio's Sunshine Laws, how to submit records requests, samples of records requests, and steps to take if you are denied records or get no response.

Additionally, included in this toolkit are some surveillance-specific PRR templates that might be of use in your investigation of government surveillance in your community.





To Whom It May Concern,

Pursuant to Ohio's open record laws, Revised Code §149.43, the following is a formal request for public records in the possession of [Office/department/governing body with potential records of interest].

For the purpose of this request, the following definitions and instructions should apply:

The term “records” includes both paper and electronically maintained information, writings, images, or data compilations— stored in any medium from which information can be obtained and further including all drafts and non-exact duplicates.

“Automatic License Plate Reader (ALPR) system” shall mean a system, software, or computer algorithm, whether used independently or in combination with one or more mobile or fixed automated cameras, that is used to convert images of license plates into computer-readable data.

Please provide copies of contracts, agreements, purchase agreements, extensions/ renewals, proposals, marketing materials, memorandums of understanding, protocols for use, right-of-way installation permits, email correspondence, and/or expenditure receipts or logs relating to the acquisition, deployment, use, or access to any Automatic License Plate Reader (ALPR) System (also/alternatively known as ALPRs, license plate readers, LPRs), including any records related to any ALPR system providers including, without limitation, Flock Safety, Motorola, Vigilant, AutoVu, Genetec, Plate Recognizer, Rekor, OpenALPR, Leonardo, and ELSAG between [mm/dd/yyyy-mm/dd/yyyy].

Our preference is to receive electronic records/ copies of records if possible. We are happy to work with you to make the transmission of electronic information as easy, inexpensive and efficient as possible. If there are any fees for copying these records, please inform me before incurring that cost.

Please send the requested records to [Your preferred email], within fourteen days of the receipt of this letter. If more time is needed, please contact me via email to discuss your anticipated response timeline. I remain open to receiving the records on a rolling basis. If you deny any or all of this request, please cite each specific exemption you feel justifies the refusal to release the information and notify me of the appeal procedures available to me under the law.

If you have any questions related to this request, please contact me via email. Thank you in advance for your assistance.

Respectfully submitted,

[Name]

[Title & Organization if applicable]



To Whom It May Concern,

Pursuant to Ohio's open record laws, Revised Code 149.43, the following is a formal request for public records in possession of the [Office/department/governing body with potential records of interest].

I hereby request copies of the following records:

- [Entity name/ organization, for example Flock] Audits, documenting all searches of license plate reader data conducted by [Office/department/governing body/city] between [mm/dd/yyyy-mm/dd/yyyy].
- [Entity name/ organization, for example Flock] Audits, documenting all searches of license plate reader data conducted by entities outside of [area of interest such as city or county] between [mm/dd/yyyy-mm/dd/yyyy].

Please send the requested records to me via email at [Your preferred email] within fourteen (14) days of receipt of this request. If more time is needed, please contact me via email to discuss your anticipated response timeline. I remain open to receiving the records on a rolling basis. If there is any cost related to the production of these documents, please notify me before incurring that cost.

If you have any questions related to this request, please contact me via email. Thank you in advance for your assistance.

Respectfully submitted,

[Name]

[Title & Organization if applicable]





To Whom It May Concern,

Pursuant to Ohio's open record laws, Revised Code 149.43, the following is a formal request for public records in possession of the [Office/department/governing body with potential records of interest].

I hereby request copies of the following records:

A. Any/all formal written policies and regulations governing the use of automatic license plate reader (ALPR) technology used by [Agency or department];

1. Any restrictions or regulations on how ALPRs are used and/or what data they collect;
2. How long ALPR data is kept, stored, or is accessible by the [Agency or department];
3. Other than [Agency or department], what other entities or people have temporary or permanent access to ALPR data collected and/or stored by [Agency or department].

B. Other than [Agency or department], what other entities or people have temporary or permanent access to ALPR data collected and/or stored by [Agency or department].

Please send the requested records to me via email at [Your preferred email] within fourteen (14) days of receipt of this request. If more time is needed, please contact me via email to discuss your anticipated response timeline. I remain open to receiving the records on a rolling basis. If there is any cost related to the production of these documents, please notify me before incurring that cost.

If you have any questions related to this request, please contact me via email. Thank you in advance for your assistance.

Respectfully submitted,

[Name]

[Title & Organization if applicable]



Public Records Requests Template for Any and All Surveillance Technology Used

To Whom It May Concern,

Pursuant to Ohio's open record laws, Revised Code 149.43, the following is a formal request for public records in possession of the [Office/department/governing body with potential records of interest].

For the purpose of this request, the following definitions and instructions should apply:

The term "records" includes both paper and electronically maintained information, e-mails, writings, graphs, charts, images, or data compilations— stored in any medium from which information can be obtained and further including all drafts and non-exact duplicates. "Surveillance technology" shall mean the specifically identified electronic surveillance device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, behavioral, or similar information or communications specifically associated with, or capable of being associated with, any specific individual or group.

We hereby request copies of the following records dated from [mm/dd/yyyy-mm/dd/yyyy]:

For each of the surveillance technologies listed below, please provide copies of any and all contracts, agreements, purchase agreements, memorandums of understanding, protocols for use, and/or expenditure receipts or logs:

- a. Automatic License Plate Readers (also/alternatively known as ALPRs, license plate readers)
- b. Body worn cameras (also/alternatively known as police body worn cameras, police body cameras)
- c. Cell site simulators (also/alternatively known international mobile subscriber identity (IMSI) catchers, Stingrays, Hailstorms)
- d. Drones (sometimes also/alternatively known as unmanned aerial vehicles)
- e. Mobile and non-mobile biometric surveillance technology, including facial-, voice-, iris-, and gait-recognition software and databases (in the case of mobile biometric surveillance technology, RapidID Program)
- f. Gunshot detection and location hardware and services (also/alternatively known as ShotSpotter)
- g. Mobile DNA capturing technology
- h. Surveillance cameras (also/alternatively known as closed circuit television cameras, CCTVs, wide-angle cameras)
- i. Predictive policing software
- j. Social media monitoring software (also/alternatively known as SMMS)
- k. Surveillance lightbulbs (also/alternatively known as surveillance enabled lightbulbs/fixtures, surveillance capable lightbulbs/fixtures)
- l. Through-the-wall sensors (also/alternatively known as through-the-wall radar)
- m. Tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network
- n. X-ray Vans (also/alternatively known as Z Backscatter Vans)

For each of the centers, facilities, operations, partnerships, programs, projects companies, and/or registries listed below, please provide copies of any and all contracts, agreements, purchase agreements, memorandums of understanding, protocols for use, and/or expenditure receipts or logs:

- a. Flock Safety
- b. Statewide Terrorism Analysis & Crime Center partner agencies
- c. Ring Doorbell partnership (sometimes also/alternatively known as Ring Neighbors partnership)
- d. BRINC Drones, Inc
- e. Recorded Future, Inc

Please send the requested records to me via email at [Your preferred email] within fourteen (14) days of receipt of this request. If more time is needed, please contact me via email to discuss your anticipated response timeline. I remain open to receiving the records on a rolling basis. If there is any cost related to the production of these documents, please notify me before incurring that cost.

If you have any questions related to this request, please contact me via email. Thank you in advance for your assistance.

Respectfully submitted,

[Name]

[Title & Organization if applicable]

Other Useful Information

[How to Pump the Brakes on Your Police Department's Use of Flock's Mass Surveillance License Plate Readers | American Civil Liberties Union](#)

[Community Control Over Police Surveillance: Technology 101 | American Civil Liberties Union](#)

[Community Control Over Police Surveillance - Resource Library | American Civil Liberties Union](#)

References

- 1 Biometrics: Environments. (2026). U.S. Customs and Border Protection. <https://www.cbp.gov/travel/biometrics/environments>
- 2 Community Control Over Police Surveillance: Technology 101. (2016, September 16). American Civil Liberties Union. <https://www.aclu.org/publications/community-control-over-police-surveillance-technology-101>
- 3 Edison, R. (2026, June 17). License Plate Cameras Now Track Your Phone, Wearables, and... Your Pets - Gadget Review. Gadget Review. <https://www.gadgetreview.com/license-plate-cameras-now-track-your-phone-wearables-and-your-pets>
- 4 ACLU. (2024, October 29). You Are Being Tracked | American Civil Liberties Union. American Civil Liberties Union. <https://www.aclu.org/you-are-being-tracked>
- 5 Finklea, K. (2024). Law Enforcement and Technology: Use of Automated License Plate Readers [Review of Law Enforcement and Technology: Use of Automated License Plate Readers]. https://www.congress.gov/crs_external_products/R/PDF/R48160/R48160.3.pdf
- 6 Inc, N. (2021, June 18). The History of License Plate Recognition Technology. Next Generation Security Concepts, Inc. <https://ngscinc.com/history-license-plate-recognition>
- 7 Flock Safety - the first public safety operating system. (2026). Flocksafety.Com. Retrieved July 10, 2026, from <https://www.flock-safety.com/>
- 8 Brewster, T. (2025, September 3). AI Startup Flock Thinks It Can Eliminate All Crime In America. Forbes. <https://www.forbes.com/sites/thomasbrewster/2025/09/03/ai-startup-flock-thinks-it-can-eliminate-all-crime-in-america/>
- 9 Meighan, S. (2025, March 28). "More of a Band-Aid": US cities canceling ShotSpotter due to cost, efficacy questions. USA Today. <https://www.usatoday.com/story/news/nation/2025/03/28/united-states-cities-shotspotter-gun-violence/82697958007/>
- 10 DeFlock. (2026). Deflock.Org. <https://deflock.org/>
- 11 Flock Safety - Richland County OH SO Transparency Portal. (2026b). Flocksafety.Com. <https://transparency.flocksafety.com/richland-county-oh-so>
- 12 Collier, K. (2025, November). Flock police cameras scan billions per month, sparking protests. NBC News. <https://www.nbcnews.com/tech/tech-news/flock-police-cameras-scan-billions-month-sparking-protests-rcna230037>
- 13 Joffe-Block, J. (2026, February 17). Why some cities are ditching their Flock license plate readers. NPR. <https://www.npr.org/2026/02/17/nx-s1-5612825/flock-contracts-canceled-immigration-surveillance-concerns>
- 14 Singh, K. (2026, May 7). Hundreds of immigration-related searches ran through Shaker Heights' Flock surveillance camera system. Cleveland.Com. <https://www.cleveland.com/news/2026/05/activists-uncover-hundreds-of-immigration-related-searches-that-ran-through-shaker-heights-flock-system.html>
- 15 Terms and conditions. (2026c). In Flocksafety.com. <https://www.flocksafety.com/legal/terms-and-conditions>
- 16 ACLU. (2017). Factsheet: The NYPD Muslim Surveillance Program. American Civil Liberties Union. <https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program>
- 17 GovFacts. (2026, January 5). GovFacts. GovFacts. <https://govfacts.org/tech-innovation/digital-rights-privacy/digital-surveillance/what-ices-new-mobile-facial-recognition-means-for-immigration-enforcement-and-privacy/>
- 18 Yu, L. (2026, April 14). Wrongful Arrests Pile Up Due to Facial Recognition Technology. American Civil Liberties Union. <https://www.aclu.org/news/privacy-technology/more-than-a-dozen-wrongful-arrests-due-to-police-reliance-on-facial-recognition-technology>
- 19 Koebler, J., & Cox, J. (2025, October 7). Police Said They Surveilled Woman Who Had an Abortion for Her "Safety." Court Records Show They Considered Charging Her With a Crime. 404Media.Co. <https://www.404media.co/police-said-they-surveilled-woman-who-had-an-abortion-for-her-safety-court-records-show-they-considered-charging-her-with-a-crime/>
- 20 Stavola, M. (2024, August 17). Kansas police chief used Flock license plate cameras 164 times to track ex-girlfriend. Wichita Eagle via Yahoo News; Yahoo News. <https://www.yahoo.com/news/kansas-police-chief-used-flock-093300946.html>
- 21 Crisolago, M. (2025, November 6). Police used 'Flock' cameras to accuse Denver woman of theft — then she had to 'prove' own innocence even though she wasn't there. Here's how. Moneywise. <https://moneywise.com/news/police-used-flock-cameras-to-accuse-denver-woman-of-theft-then-she-had-to-prove-own-innocence-even-though-she-wasnt-there-heres-how>
- 22 Oyez. (2019). United States v. Jones. Oyez. <https://www.oyez.org/cases/2011/10-1259>
- 23 Oyez. (2019). Carpenter v. United States. Oyez. <https://www.oyez.org/cases/2017/16-402>
- 24 Chatrue v. United States, (United States Supreme Court June 29, 2026). https://www.supremecourt.gov/opinions/25pd-f/25-112_0am4.pdf

- 24 Koebler, J. (2025, January 7). Researcher Turns Insecure License Plate Cameras Into Open Source Surveillance Tool. 404 Media. <https://www.404media.co/researcher-turns-insecure-license-plate-cameras-into-open-source-surveillance-tool/>
- 25 Maass, D. (2019, March 19). Here's Why You Can't Trust What Cops and Companies Claim About Automated License Plate Readers. Electronic Frontier Foundation. <https://www.eff.org/deeplinks/2019/03/heres-why-you-cant-trust-what-cops-and-companies-claim-about-automated-license>
- 26 Geniusz, K. (2026, April 28). Central Ohio police departments have spent nearly \$2 million on Flock license plate cameras. WOSU Public Media. <https://www.wosu.org/politics-government/2026-04-28/central-ohio-police-departments-have-spent-nearly-2-million-on-flock-cameras>
- 27 McDonnell, S. (2026, July 15). Cleveland to keep Flock cameras after City Council vote. Cleveland.Com. <https://www.cleveland.com/news/2026/07/cleveland-to-keep-flock-cameras-after-city-council-vote.html> <https://www.cleveland.com/news/2026/06/cleveland-council-committee-rejects-250000-flock-surveillance-contract-renewal-amid-privacy-concerns.html>
- 28 Marshall, A. (2026, May 20). Some residents say “Flock No” to surveillance tech as Cleveland mulls contract renewal. Ideastream Public Media. <https://www.ideastream.org/government-politics/2026-05-20/some-residents-say-flock-no-to-surveillance-tech-as-cleveland-mulls-contract-renewal>
- 29 Geniusz, K. (2026, April 28). Central Ohio police departments have spent nearly \$2 million on Flock license plate cameras. WOSU Public Media. <https://www.wosu.org/politics-government/2026-04-28/central-ohio-police-departments-have-spent-nearly-2-million-on-flock-cameras>
- 30 U.S. Department of Justice. “Agency Requirements.” Overview of the Privacy Act of 1974, 2020 Edition, Office of Privacy and Civil Liberties, 2020, <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/agency-requirements>.
- 31 Stanley, C. M., Jay. (2023, February 13). How to Pump the Brakes on Your Police Department's Use of Flock's Mass Surveillance License Plate Readers | ACLU. American Civil Liberties Union. <https://www.aclu.org/news/privacy-technology/how-to-pump-the-brakes-on-your-police-departments-use-of-flocks-mass-surveillance-license-plate-readers>
- 32 Villarreal Martinez, D. (2026, May 12). Newport officials are happy with Flock Safety cameras so far, but residents are concerned. WVXU. <https://www.wvxu.org/local-news/2026-05-12/newport-flock-safety-cameras-concerns>
- 33 The FBI Wants to Buy Nationwide Access to License Plate Readers. (2026, May 23). The Free Thought Project. <https://thefree-thoughtproject.com/government-surveillance/the-fbi-wants-to-buy-nationwide-access-to-license-plate-readers>
- 34 Bio, S. (2026). AI Is Watching Your Every Move on the Road. These State Laws Are Pushing Back. CNET. <https://www.cnet.com/home/security/ai-is-watching-your-every-move-on-the-road-these-state-laws-are-pushing-back/>
- 35 Legislative Information System. (2024, June 14). Official government website of the Illinois General Assembly. Ilga.Gov. <https://www.ilga.gov/Legislation/publicacts/view/095-0994>
- 36 XXI Motor Vehicles, 261:75-b (2007). <https://gc.nh.gov/rsa/html/XXI/261/261-75-b.htm>
- 37 Marshall, A. (2026b, May 20). Some residents say “Flock No” to surveillance tech as Cleveland mulls contract renewal. Ideastream Public Media. <https://www.ideastream.org/government-politics/2026-05-20/some-residents-say-flock-no-to-surveillance-tech-as-cleveland-mulls-contract-renewal>
- 38 Tedtman, E. (2025, May 12). Police Surveillance and Civil Liberties - ACLU of Ohio. ACLU of Ohio. <https://www.acluohio.org/news/police-surveillance-and-civil-liberties/>
- 39 Rogelberg, S. (2026, June 3). Ohio city workers are covering automated license plate readers with trash bags as officials sound the alarm on ‘egregious violations’ of privacy. Fortune. <https://fortune.com/2026/06/03/why-are-ohio-city-workers-covering-flock-cameras-immigration-enforcement-data-sharing-policy-violations/>
- 40 Community Control Over Police Surveillance | American Civil Liberties Union. (2024, November 21). American Civil Liberties Union. <https://www.aclu.org/community-control-over-police-surveillance>
- 41 Grzegorek, V. (2021, January 21). Scene sues city of Cleveland over Police use of force records. Scene. Cleveland Scene. <http://www.clevescene.com/scene-and-heard/archives/2021/01/21/scene-sues-city-of-cleveland-over-police-use-of-force-records>

Appendix

U.S. Cities That Have Ended Their Use of Flock (and other) ALPRs

City	Date
Ft. Collins, CO	6/17/26
Columbia Heights, MN	6/9/26
Grand Chute, WI	6/3/26
Fort Wayne, IN	5/27/26
Edmonds, WA	5/26/26
Fitchburg, WI	5/25/26
Menominee, MI	5/18/26
Pittsboro, NC	5/12/26
Bandera, TX	5/12/26
El Cerrito, CA	5/6/26
Appleton, WI	5/5/26
Dayton, OH	5/2/26
Oshkosh, WI	4/23/26
Dane County, WI	4/19/26
Sturgeon Bay, WI	4/15/26
Bloomington, IN	4/15/26
Tompkins County, NY	4/14/26
Attleboro, MA	3/22/26
Saranac Lake, NY	3/9/26
Ithaca, NY	3/8/26

City	Date
Coralville, IA	2/24/26
Denver, CO	2/23/26
Lynnwood, WA	2/23/26
South Tucson, AZ	2/19/26
Seneca, MO	2/19/26
Pine Plains, NY	2/3/26
Mountain View, CA	2/3/26
Prosser, WA	1/30/26
Watertown, MA	1/28/26
Los Altos Hills, CA	1/27/26
Syracuse, NY	1/26/26
Greenfield, MA	1/22/26
Natick, MA	1/21/26
Santa Cruz, CA	1/13/26
Bend, OR	1/8/26
Walla Walla, WA	1/6/26
Staunton, VA	12/22/25
Flagstaff, AZ	12/19/25
Charlottesville, VA	12/18/25
San Marcos, TX	12/15/25

City	Date
Poestenkill, NY	12/13/25
Longmont, CO	12/10/25
Cambridge, MA	12/10/25
Lane County, OR	12/10/25
Salt Lake City, UT	12/10/25
Richmond, CA	12/9/25
Warren, RI	12/9/25
Eugene, OR	12/5/25
Springfield, OR	12/5/25
Mountlake Terrace, WA	12/4/25
Woodburn, OR	11/13/25
Skamania County, WA	11/13/25
Verona, WI	11/11/25
Hillsborough, NC	11/10/25
Hays County, TX	10/14/25
Sedona, AZ	9/10/25
Evanston, IL	8/26/25
Oak Park, IL	8/7/25
Scarsdale, NY	8/6/25
Austin, TX	6/6/25

Acknowledgements:

The ACLU of Ohio staff is responsible for the contents of this report, which was researched and written by Raegan Elliott, Ohio University Pre-Law Program Fellow, with support from Sean McCann, Policy Strategist and Jocelyn Rosnick, Chief Policy & Advocacy Officer. Celina Coming, Chief Public Relations Officer, Gary Daniels, Legislative Director, Collin Marozzi, Advocacy Director, and Natalie Johnson, Advocacy Strategist, provided editorial support and technical edits. Sara Tkac, Digital Design Strategist, provided the report design. Additional support was provided by Riley Taylor, Advocacy Strategist.

The ACLU of Ohio team would also like to thank Chad Marlow, Senior Policy Counsel (Privacy, Surveillance & Technology), ACLU, for his guidance on mass surveillance issues.