

— AUTOMATED LICENSE PLATE READERS · MASS SURVEILLANCE · DISPARATE IMPACT · METHODS OF ADMINISTRATION · MEANINGFUL ACCESS · UNLAWFUL EAVESDROPPING AND SURVEILLANCE · CONTINENTAL GEOFENCE · SUBSCRIPTION SURVEILLANCE · VAN BUREN V. UNITED STATES · PARANOIA-SPECTRUM CONDITIONS · LAW ENFORCEMENT INSIDER THREAT · GOVERNMENT-RELATED DATA

Already Illegal

Flock Safety

and the six bodies of existing law nobody is applying

Everyone is drafting the next surveillance statute. Six that already reach this network are sitting unused, and not one of them is a privacy law.

WHERE THE ARGUMENT IS STUCK

Every fight about these cameras is a fight about the next bill

Advocates describe a surveillance system of unprecedented reach. Legislators draft privacy bills. The vendor says the bills would slow down police work. Everyone argues as though nothing on the books today touches any of it.

Washington

Passed a twenty-one day retention rule in March. The vendor announced it had already begun complying.

California

A governor vetoed one bill. The replacement sits in a committee, with the governor's office declining to take a position.

Everywhere else

Michigan introduced one this month. A member of Congress promised one on social media. Most states have nothing.

SOURCES Wash. Laws of 2026 (signed Mar. 30, 2026); Cal. S.B. 274 (2025) (vetoed Oct. 2025).

What it means: The legislative path is slow, thin, and easy for a vendor to absorb. That is a reason to look at what is already enacted, not a reason to wait.

THE CLAIM

Six laws already reach this, and each one has a different defendant

- 1 The city that bought it**
Disability antidiscrimination law asks whether a public entity's own administrative choices close its own program to a protected class.
- 2 Whoever does the watching**
Observing a person in a private space without their consent is a felony in Georgia and in most states.
- 3 The seller**
Consumer protection law covers what the company told buyers and how badly it secured the product.
- 4 Whoever handed over access**
A city cannot give a vendor a permission it never held.
- 5 The intruder**
Anyone who opens a camera on a pole is trespassing on a computer.
- 6 The data itself**
The government already classified this category of location data as a risk to national security.

SOURCES 42 U.S.C. § 12132; 29 U.S.C. § 794(a); Ga. Code Ann. § 16-11-62(2); 15 U.S.C. § 45(a)(1), (n); 18 U.S.C. § 1030(a)(2)(C); 28 C.F.R. pt. 202.

What it means: Not one of these is a privacy statute. A privacy law asks whether a person agreed to be watched. These ask whether a particular actor was allowed to do a particular thing, which courts answer every day.



The statute everyone reaches for

Why the children's privacy law does not touch a camera on a pole

When children appear in a surveillance story the reflex is COPPA. Understanding why it fails is what makes the other six visible.

THE WRONG TOOL, AND WHY THAT MATTERS

COPPA is a permission slip, and there is nobody to ask

The statute does one thing. If you run a service aimed at children, or you know you are collecting from a child under thirteen, you must tell the parents and get their agreement before you collect. The 2025 amendments widened what counts as personal information. They did not change the shape.

Collected online

The three examples of collection all describe a child typing something in, publishing something, or being tracked across websites. A camera photographing a body in a room is none of those.

Directed to children

The audience test weighs who the users are. The users of a plate reader network are police departments. A camera pointed at a playground is aimed at children. It is not offered to them.

No addressee

The only remedy is notice to a parent before collection. On a public pole there is no moment at which anyone could be asked.

SOURCES 15 U.S.C. § 6502(a)(1), (b)(1)(A); 16 C.F.R. § 312.2 (2026); Children's Online Privacy Protection Rule, 90 Fed. Reg. 16918 (Apr. 22, 2025).

What it means: Consent statutes need a moment of contact and ambient capture has none. So stop looking for a consent law and look for laws about what an actor may do.



The city that bought it, and the act of watching

Disability antidiscrimination law and state criminal surveillance law

Two laws, two defendants. The municipality that procured and sited the network, and whoever sat down and looked through it.

THE PROGRAM IS THE STREET ITSELF

Roads are a public program, and the rule asks about effect, not intent

Title II says a public entity may not deny a disabled person the benefits of its services, programs, or activities. Courts settled long ago that maintaining and building the public right of way is one of those programs. Where the cameras were bought with federal grant money, Section 504 gives a second, nearly identical claim.

“criteria or methods of administration ... that have the purpose or effect of defeating or substantially impairing accomplishment of the objectives of the public entity's program with respect to individuals with disabilities”

28 C.F.R. § 35.130(B)(3)

How long reads are kept, who else in the country can search them, and how loudly the deployment is advertised are administrative choices. The city picked them and the city can change them. And the city cannot hide behind the vendor, because the regulation reaches discrimination carried out through contracts and licensing.

SOURCES 42 U.S.C. § 12132; 29 U.S.C. § 794(a); *Barden v. City of Sacramento*, 292 F.3d 1073, 1076 (9th Cir. 2002); *Frame v. City of Arlington*, 657 F.3d 215, 225–26 (5th Cir. 2011) (en banc); 28 C.F.R. §§ 35.130(b)(1), (b)(3).

What it means: Nobody has to prove the city meant to harm anyone. The question is whether the way it runs the program has that result, and hiring a contractor does not move the liability.

THE MECHANISM IS CLINICAL, NOT RHETORICAL

The treatment depends on the belief turning out to be false

The leading model treats a persecutory belief as a threat belief kept alive by avoidance. Treatment works by getting the patient to test the belief against the world and find it wrong.

A controlled trial isolated the active ingredient. Patients who tested their predictions and dropped their safety behaviors showed a twenty-two percent drop in how strongly they held the belief. Exposure alone did much less.

Now put that patient on a street where the city records where every car goes and keeps it searchable by strangers in other states. The belief that she is being recorded, and that strangers can retrieve it, is true. There is nothing left to disconfirm.

SOURCES Daniel Freeman, *Persecutory Delusions: A Cognitive Perspective on Understanding and Treatment*, 3 *Lancet Psychiatry* 685 (2016); Daniel Freeman et al., *Virtual Reality in the Treatment of Persecutory Delusions*, 209 *Brit. J. Psychiatry* 62 (2016).

What it means: Everyone else loses comfort. This class loses a working treatment, because the therapy needs the belief to be false and the city just made it true.

WHAT A COURT WOULD ACTUALLY ORDER

Settings, not demolition

Keep less

Turn a permanent archive into a short rolling buffer, with an automatic purge.

Every one of those changes how the network operates and not one takes down a camera, which is what makes them reasonable modifications rather than a demand to abolish the program.

On money, a 2026 decision barred recovery for emotional distress under Title II but preserved compensatory damages for lost opportunities. So plead the job not taken and the appointment not attended, not the fear. An injunction, which is the relief that matters against a network, is untouched.

Draw quiet zones

Suppress reads around clinics, supportive housing, and peer support centers.

Log every search

Record who ran what and why, in a field that cannot be satisfied with nonsense.

Expire the hotlists

No entry that watches a person forever without review.

SOURCES 28 C.F.R. § 35.130(b)(7)(i); Alexander v. Choate, 469 U.S. 287, 301 (1985); Alexander v. Sandoval, 532 U.S. 275, 289, 293 (2001); Payan v. L.A. Cmty. Coll. Dist., 169 F.4th 971, 977–79 (9th Cir. 2026); Cummings v. Premier Rehab Keller, P.L.L.C., 596 U.S. 212 (2022).

What it means: Courts grant orders they can supervise, and these are all supervisable. Where circuits disagree about who may sue, a complaint to the federal grant-maker works either way.

THE OPERATIVE WORDS

One sentence, a felony, and it never mentions cameras

“It shall be unlawful for any person, through the use of any device, without the consent of all persons observed, to observe, photograph, or record the activities of another which occur in any private place and out of public view.”

GA. CODE ANN. § 16-11-62(2)

A violation is a felony carrying one to five years, a fine up to ten thousand dollars, or both, and anything obtained in violation of it cannot be used as evidence in a Georgia court. Notice the verb. To observe. Nothing has to be recorded, kept, or shared. Watching completes the crime.

And the consent required is that of all persons observed. Not the owner of the property, not the lessee, not whoever signed the camera agreement. When a private facility lets a department see its interior cameras, the facility has consented for the facility. The people in the room consented to nothing.

SOURCES Ga. Code Ann. § 16-11-62(2); id. § 16-11-62(6); id. § 16-11-69; id. § 16-11-67; id. § 16-11-60(3).

What it means: Live viewing alone is the offense, there is no recording requirement to argue about, and signatures on the camera contract are legally irrelevant to the people the camera points at.

THE EXCEPTIONS, AND THE TRAP INSIDE ONE

The property owner exception argues against itself

1 Owners and occupiers, but only sometimes

A property owner may use cameras for security only in areas where there is no reasonable expectation of privacy. So if the room is private, the owner's own cameras fall outside the exception too. The circle closes against the defense.

2 Officers, in person

A law enforcement officer acting in official duties may observe activities occurring in that officer's presence. A sales demonstration is not official duty, and a remote video feed is not presence.

3 Where this gets litigated

The one contested element is whether a space is private and out of public view. Georgia construes the statute strictly, so interior rooms and changing areas are strong ground and an open floor is weak. Pick the room, not the building.

SOURCES Ga. Code Ann. § 16-11-62(2)(A)–(D); Gary v. State, 338 Ga. App. 403, 406–09 (Ga. Ct. App. 2016); Rutter v. Rutter, 294 Ga. 1, 3–5 (2013).

What it means: Two of the four exceptions cannot cover a vendor at all, and the third only protects cameras where nobody expects privacy, which is the opposite of the rooms at issue.



The seller, and the access

Consumer protection law and the ordinary law of contract and agency

What the company said to buyers, how badly it locked the product, and whether anyone had the authority to hand over the keys.

TWO THEORIES, AND ONE DEFENSE THAT FAILS

What was said, and what was built

Deception

The company told the press it had no federal contracts, so federal sharing was not an issue. Its own disclosure page now lists a Customs and Border Protection pilot from May to August 2025 and a Homeland Security Investigations pilot from March to May 2025. Those statements were made to city councils in open session, during the vote.

The Third Circuit settled that the unfairness power covers data security. The holding that matters here is narrower: a company's conduct need not be the closest cause, and a criminal third party does not break the chain where the company made the harm foreseeable. A button sequence on the back of a pole-mounted camera opened a diagnostic access point, and root followed in under thirty seconds. A researcher found sixty-seven live feeds on the open internet with no login at all.

Unfairness

Substantial harm, not reasonably avoidable, not outweighed by the benefits. A driver cannot decline to be photographed by a camera whose location is not published, and cannot know the feed is open.

SOURCES 15 U.S.C. § 45(a)(1), (n); FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 246, 255–56 (3d Cir. 2015); LabMD, Inc. v. FTC, 894 F.3d 1221, 1236 (11th Cir. 2018).

What it means: The company cannot point at whoever walked through the door it left open. The LabMD decision vendors cite is about how narrowly an order must be written, not about whether the agency has the power.

A PERMISSION YOU NEVER HELD

The Supreme Court settled this in 1964

A private institution is asked to add its interior cameras to a city network. It refuses the open-ended version. The department writes back narrowing the request to one purpose, commonly live response to an emergency. On that written promise the institution agrees. What the department received was a license with terms, and a later agreement with a vendor operates only on what the department holds.

“It was a right, therefore, which only the petitioner could waive by word or deed, either directly or through an agent.”

STONER V. CALIFORNIA, 376 U.S. 483, 489 (1964)

The Court drew the line precisely. A guest gives implied permission for maids, janitors, and repairmen to come in and do their jobs, and that permission does not extend to authorizing a search. A facility granting camera access for emergency response is that permission. A salesperson opening the feed to close a deal is that search.

SOURCES Stoner v. California, 376 U.S. 483, 488–89 (1964); Illinois v. Rodriguez, 497 U.S. 177, 188–89 (1990); Ga. Code Ann. § 10-6-51; Omni Builders Risk, Inc. v. Bennett, 313 Ga. App. 358, 360–61 (Ga. Ct. App. 2011); Ga. Code Ann. § 13-3-44(a); Kemira, Inc. v. Williams Investigative & Sec. Servs., Inc., 215 Ga. App. 194, 198–99 (Ga. Ct. App. 1994).

What it means: Letting someone in to do a specific job is not letting them do anything they like, and apparent authority fails because the manifestations must come from the institution, which never made any to the vendor.

IV

The machine, the data, and the gap

Computer crime law and the national security rule, plus the one place this argument yields

Two more laws reach this, and one hole runs straight through the middle of them.

IT CATCHES THE LADDER AND MISSES THE BADGE

A Georgia sergeant sold a plate lookup and the Supreme Court let him go

Federal law makes it a crime to intentionally access a computer without authorization and obtain information from it. Somebody who walks up to a pole, opens the diagnostic access point, and takes root has no permission at any point. The vendor's answer, that this requires physical access and hardware knowledge, does not survive its own product. The cameras are on public poles at ladder height.

Nathan Van Buren was a police sergeant in Georgia. A man working with the FBI offered him about five thousand dollars to run one license plate through the state law enforcement database. He used his own valid login and ran it.

The Supreme Court held he had not exceeded his authorized access. The test is whether you are allowed into that area of the system, not why you went in. Improper purpose is not the question. Justice Thomas would have held the opposite and did not carry the Court.

SOURCES 18 U.S.C. § 1030(a)(2)(C), (e)(2)(B); Van Buren v. United States, 593 U.S. 374, 378, 390, 400 (2021) (Thomas, J., dissenting); 18 U.S.C. § 666(a)(1)(B), (b); Snyder v. United States, 603 U.S. 1 (2024).

What it means: An officer with a legitimate account who enters a plate for money has not committed a federal computer crime. That is the gap, and it is the only one. Federal bribery might reach it, but its dollar threshold attaches to the agency's underlying deal and it has never been tried on these facts.

WHAT IS ACTUALLY BEING PURCHASED

Not a lookup. A subscription.

A lookup

Answers where a vehicle has been. One question, one answer, paid once.

A hotlist entry

Answers where it is, from now on. No judge reviews the entry and nothing makes it expire.

Non-entry

Paying to make sure a particular plate never alerts. Counter-surveillance, and to some buyers worth more than tracking.

Once an entry exists, every camera in the network checks every passing vehicle against it and pushes an alert to a phone with an image and a location. The vendor markets that sequence as the product. After the first payment, the cost of continuing is zero.

That is the difference between hiring an investigator for a day and installing one permanently, and it is why a gap in the computer crime statute matters more than it sounds.

SOURCES Van Buren v. United States, 593 U.S. 374, 390 (2021); 18 U.S.C. § 1030(a)(2)(C).

What it means: One bribe buys a permanent feed rather than a single answer, and nothing in the system makes that entry expire or come back for review.

THE RULE, IN ITS OWN WORDS

736 boxes on a map, and no minimum amount

“any precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List”

28 C.F.R. § 202.222(A)(1)

The Attorney General made that determination because such data can reveal what happens at federally controlled locations, including the work sites of people who hold national security positions. Precise means within one thousand meters. The list is published, with the corner coordinates of every area.

There is no threshold. A single reading counts, because a single reading can carry the insight. The executive branch decided this in a binding rule and wrote down why.

SOURCES Exec. Order No. 14117, 89 Fed. Reg. 15421 (Mar. 1, 2024); 90 Fed. Reg. 1636 (Jan. 8, 2025) (codified at 28 C.F.R. pt. 202); 28 C.F.R. §§ 202.222(a)(1), 202.242, 202.1401.

What it means: The government has already agreed on the record that location data around these sites is a security problem, which makes this rule evidence as much as it is a cause of action.

THE BUSINESS MODEL IS INSIDE THE DEFINITION

Selling subscription access to somebody else's camera reads

The rule defines data brokerage as selling data, or licensing access to it, where the person receiving it did not collect it from the people it describes. The Department's own worked example is an organization that keeps a database and sells annual memberships to search it. That is precisely the product.

1 Selling to a covered person

Brokerage with a country of concern, or anyone primarily resident in one, is prohibited outright.

2 Selling to any foreign person

No hostile country needed. If any foreign person can reach this data, the operator must contractually bar onward sale and report suspected breaches within fourteen days. Not having the clause is itself the violation.

3 Hiring a covered vendor

Any service agreement, cloud included, giving a covered person access is a restricted transaction allowed only if the security requirements are met.

SOURCES 28 C.F.R. §§ 202.214(a), 202.214(b)(3), 202.301(a), 202.211(a)(4), 202.302(a)–(b), 202.258(a), 202.401, 202.248, 202.230(b)(1).

What it means: The subscription business is the exact thing the rule calls data brokerage. What the rule does not reach is theft, so stolen logins sold on a criminal forum fall outside it even though they create the same harm.

WHAT HAPPENED WHEN THE TWO PUBLIC DATASETS WERE JOINED

504 readers inside the fences, 11,992 on the approach

504

READERS INSIDE TIGHTLY
DRAWN FEDERAL GEOFENCES

Seventy-four of the 736 published areas have at least one reader inside the boundary. Strip out the forty-one oversized polygons, some hundreds of kilometres across, and fifty-five tightly drawn areas still hold 504 readers inside the line.

Then widen the ring. Within two kilometres of an enumerated area, 4,656 readers. Within five, 7,660. Within ten, 11,992.

The rule fenced the destinations. The network holds the roads to them, and that is where a pattern of life is actually built.

SOURCES 28 C.F.R. § 202.1401 tbl.1 (published corner coordinates for all 736 areas); OpenStreetMap, retrieved Aug. 10, 2026 (23,946 nodes tagged as automated plate readers).

What it means: Both datasets are public, so anyone can rerun this. The camera map is volunteer-built, so it proves cameras are there and can never prove they are absent. Every number is a floor.

ONE ZONE

The densest is 2.14 square kilometres, and it is the Pentagon

The published corners enclose a rectangle roughly 1.5 by 1.4 kilometres on the Virginia bank of the Potomac. Rendered over satellite imagery it resolves to the Pentagon reservation, with Arlington National Cemetery on the west edge and the Boundary Channel on the east.

Eleven mapped readers sit inside it, and they are not scattered. Two at the northern approach, two at the eastern river crossing, three on the interior ramps, four at the southern parking interchange. They sit on the ways in and out.

The obvious objection is that a plate identifies a car, not a person. The rule answers it first, because this category of data does not have to be linked to anyone at all. The research answers it second: in a set of 1.5 million people, four points in time and space identified ninety-five percent of individuals uniquely.

SOURCES 28 C.F.R. § 202.1401 tbl.1 (Area ID 605); id. § 202.222(a)(1); Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 Sci. Reps. 1376 (2013).

What it means: The government drew this box itself and said why. A commercial network selling searchable access runs eleven cameras inside it, positioned on the entrances.

THE HONEST OBSTACLES

Seven places this argument has to fight

- 1 Effects claims have a ceiling**
Choate refused to make every neutral policy with uneven effects presumptively unlawful, and circuits divide on who may enforce the effects regulation.
- 2 Private place is contested**
Georgia construes its criminal statute strictly, so an open floor is much harder than an interior room.
- 3 Security orders must be specific**
LabMD vacated an order for lack of specificity, which means naming the exact controls.
- 4 Apparent authority will be argued**
And answered, because the manifestations must come from the party that held the right.
- 5 The bribery threshold is untested**
Its dollar figure attaches to the agency's underlying transaction, and gratuities sit outside the statute.
- 6 The data rule covers deals, not theft**
The clearest harm sits just outside its prohibitions.
- 7 The camera map is incomplete**
Volunteer data proves presence and never absence.

SOURCES Alexander v. Choate, 469 U.S. 287, 298–99 (1985); Gary v. State, 338 Ga. App. 403, 406 (Ga. Ct. App. 2016); LabMD, Inc. v. FTC, 894 F.3d 1221, 1236 (11th Cir. 2018); Snyder v. United States, 603 U.S. 1 (2024); 28 C.F.R. § 202.230(b)(1).

What it means: Every one of these is a question a court already knows how to answer. Not one of them requires a legislature to act first.

THE CONCLUSION

Six laws, none written for this, all in force now

The purchase is reachable under the disability statutes. The watching is a felony in Georgia and its analogues. What the seller said and how it secured the product are reachable under Section 5. Access beyond the scope of the camera owner's permission is reachable in contract and agency law. The intruder is reachable under the computer crime statute. And the location data itself is already classified by the executive branch as a national security category.

One real gap exists, and it is the bought insider. That is what a legislature should be drafting toward, and it is not what any current bill addresses.

The last observation is for the audience that has never cared about any of this. The people who will decide whether this infrastructure continues are inside its coverage. The tool cannot tell them apart from anyone else. It was not built to.

SOURCES 42 U.S.C. § 12132; 29 U.S.C. § 794(a); Ga. Code Ann. § 16-11-62(2); 15 U.S.C. § 45(a)(1), (n); 18 U.S.C. § 1030(a)(2)(C); 28 C.F.R. pt. 202; *Van Buren v. United States*, 593 U.S. 374 (2021).

What it means: Six enforcement routes are available today. The one hole is the officer who is paid, and closing it is a smaller drafting job than any bill now pending.

Travis Gilly, *Already Illegal: Flock Safety and the Six Bodies of Existing Law Nobody Is Applying* (working draft v2, August 2026).

CASES

Alexander v. Choate, 469 U.S. 287 (1985).

Alexander v. Sandoval, 532 U.S. 275 (2001).

Barden v. City of Sacramento, 292 F.3d 1073 (9th Cir. 2002).

Cummings v. Premier Rehab Keller, P.L.L.C., 596 U.S. 212 (2022).

Federal Trade Commission v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

Frame v. City of Arlington, 657 F.3d 215 (5th Cir. 2011) (en banc).

Gary v. State, 338 Ga. App. 403 (Ga. Ct. App. 2016).

Hunt v. Washington State Apple Advertising Commission, 432 U.S. 333 (1977).

Illinois v. Rodriguez, 497 U.S. 177 (1990).

Kemira, Inc. v. Williams Investigative & Security Services, Inc., 215 Ga. App. 194 (Ga. Ct. App. 1994).

LabMD, Inc. v. Federal Trade Commission, 894 F.3d 1221 (11th Cir. 2018).

CASES (CONTINUED)

Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992).
Omni Builders Risk, Inc. v. Bennett, 313 Ga. App. 358 (Ga. Ct. App. 2011).
Payan v. Los Angeles Community College District (Payan I), 11 F.4th 729 (9th Cir. 2021).
Payan v. Los Angeles Community College District (Payan II), 169 F.4th 971 (9th Cir. 2026).
Rutter v. Rutter, 294 Ga. 1 (Ga. 2013).
Snyder v. United States, 603 U.S. 1 (2024).
Somerville v. White, 337 Ga. App. 414 (Ga. Ct. App. 2016).
Stoner v. California, 376 U.S. 483 (1964).
Tennessee v. Lane, 541 U.S. 509 (2004).
Van Buren v. United States, 593 U.S. 374 (2021).

STATUTES AND REGULATIONS

Americans with Disabilities Act of 1990, 42 U.S.C. §§ 12101–12213.
Bribery concerning programs receiving Federal funds, 18 U.S.C. § 666.
Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506.
Children's Online Privacy Protection Rule, 16 C.F.R. pt. 312.
Computer Fraud and Abuse Act, 18 U.S.C. § 1030.
Federal Trade Commission Act, 15 U.S.C. § 45.
Georgia Code Annotated §§ 16-11-60 to 16-11-69.
Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 28 C.F.R. pt. 202.
Rehabilitation Act of 1973, Section 504, 29 U.S.C. § 794.

ADMINISTRATIVE AND REGULATORY MATERIALS

SECONDARY AUTHORITIES

American Civil Liberties Union. (2026). *Flock Safety credibility lost as it repeatedly lies to city councils, police departments, and public across the country*.
<https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/flock-safety-credibility-lost-as-it-repeatedly-lies-to-city-councils-police-departments-and-public-across-the-country>.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the crowd: The privacy bounds of human mobility. *Scientific Reports*, 3, 1376.

Flock Safety. (n.d.). *Does Flock share data with ICE?*<https://www.flocksafety.com/blog/does-flock-share-data-with-ice>.

Freeman, D. (2016). Persecutory delusions: A cognitive perspective on understanding and treatment. *Lancet Psychiatry*, 3, 685.

Freeman, D., Bradley, J., Antley, A., Bourke, E., DeWeever, N., Evans, N., ... Clark, D. M. (2016). Virtual reality in the treatment of persecutory delusions. *British Journal of Psychiatry*, 209, 62.

Gaines, J. (2026). *Finding 67 Flock Safety live PTZ camera/LPR feeds and debug web interfaces accidentally exposed without authentication to the internet*. GainSec.
<https://gainsec.com/2026/01/09/bird-hunting-season-finding-67-live-camera-feeds-and-debug-web-interfaces-accidentally-exposed-by-flock-safety/>.

Koebler, J. (2025). Illinois cops gave ICE access to more than 5,000 surveillance cameras nationwide. *404 Media*.

Lincoln, T. M., & Peters, E. (2019). A systematic review and discussion of symptom specific cognitive behavioural approaches to delusions and hallucinations. *Schizophrenia Research*, 203, 66.

Pereira, G., & Raetzsch, C. (2022). From banal surveillance to function creep: Automated license plate recognition (ALPR) in Denmark. *Surveillance & Society*, 20(3), 265.

Schneider, J. (2025). Big Brother left the door open: Flock's AI surveillance cameras exposed to the internet. *PetaPixel*.

University of Washington Center for Human Rights. (2025). *Leaving the door wide open: Flock surveillance systems expose Washington data to immigration enforcement*.
<https://jsis.washington.edu/humanrights/2025/10/21/leaving-the-door-wide-open/>.