

WA Surveillance Watch Template

LEGAL CONTEXT FOR SURVEILLANCE CAMERA PUBLIC RECORDS REQUESTS

Recent Washington State Court Ruling & Federal Access Concerns

November 2024

EXECUTIVE SUMMARY

In November 2024, a Washington State Superior Court judge ruled that data collected by automated surveillance cameras, including Flock Safety ALPR systems, qualifies as public records under the Washington Public Records Act (RCW 42.56). This landmark decision strengthens the public's right to access surveillance data collected by law enforcement agencies across Washington State.

Additionally, a University of Washington report revealed that federal immigration enforcement agencies had accessed Washington's surveillance camera networks, often without local agencies' knowledge, raising serious concerns about state sovereignty and civil liberties.

THE SKAGIT COUNTY SUPERIOR COURT RULING

Case Background

Case: *Rodriguez v. City of Sedro Woolley and City of Stanwood*

Court: Skagit County Superior Court

Judge: Elizabeth Yost Neidzwski

Date: November 7, 2024

Parties: - **Plaintiff:** Jose Rodriguez, a tattoo artist and Oregon resident who works in Washington - **Defendants:** Cities of Sedro Woolley and Stanwood

What Happened

Jose Rodriguez filed public records requests with dozens of Washington police agencies seeking images captured by Flock Safety automated license plate reader (ALPR) cameras. Many agencies complied with his requests. However, the cities of Sedro Woolley and Stanwood refused to provide the records and sued Rodriguez in civil court to block his requests.

The cities argued that: 1. Releasing the surveillance images would violate individuals' privacy 2. The data could enable malicious actors such as stalkers 3. The images should be exempt from public disclosure

The Court's Ruling

Judge Neidzowski **rejected** the cities' arguments and ruled that:

"The Flock data do qualify as public records subject to the Public Records Act."

Key Findings:

1. **Broad and Indiscriminate Collection:** The judge found that the scope of Flock surveillance was "so broad and indiscriminate" — with most images capturing people not suspected of any crime — that the data must be released under public records law.
2. **No Privacy Exemption:** The court determined that collecting data on everyone indiscriminately does not create a privacy exemption under RCW 42.56.
3. **Public Accountability:** The ruling emphasizes that when government surveillance affects the general public, transparency and accountability through public records access is paramount.
4. **Limited Scope:** The judge clarified that her ruling addressed only Public Records Act issues, not other legal controversies surrounding ALPR technology.

Immediate Impact

Following the ruling: - **Both cities turned off their Flock camera systems** - Multiple other Washington cities paused or delayed Flock camera deployments pending the court decision - Mountlake Terrace delayed installation until "the current legal situation sorts itself out" - Woodway delayed voting on a Flock contract - The ruling set precedent affecting dozens of Washington police departments using similar technology

UNIVERSITY OF WASHINGTON REPORT: FEDERAL ACCESS CONCERNS

Report Details

Title: "Leaving the Door Wide Open: Flock Surveillance Systems Expose Washington Data to Immigration Enforcement"

Author: University of Washington Center for Human Rights

Date: October 2024

Key Findings

The report revealed **three types of access** to Washington State surveillance data by federal agencies:

1. "Front Door" Access (Direct Sharing)

- **At least 8 Washington law enforcement agencies** enabled direct, 1:1 sharing of their Flock networks with U.S. Border Patrol
- This occurred during 2025

- Some agencies claim they were unaware they had granted this access

2. “Back Door” Access (Unauthorized)

- **At least 10 Washington police departments** had their data accessed by Border Patrol through a “pilot program” that was not previously disclosed by Flock Safety
- These agencies had NOT explicitly authorized Border Patrol access
- This occurred from at least May through August 2025

3. “Side Door” Access (Proxy Searches)

- Law enforcement agencies in Washington State conducted searches of Flock data **on behalf of** ICE or Border Patrol
- Law enforcement agencies from **other states** conducted numerous searches of Washington surveillance data
- One particularly concerning case: A Texas police officer searched Washington data (including Yakima and Prosser) to track a woman who had a self-administered abortion

Agencies That Discovered Unauthorized Access

Auburn and Lakewood police departments stated publicly that they:

- Were unaware of Border Patrol’s access to their systems -
- Immediately revoked access upon discovering it -
- Had “National Lookup” features enabled, which facilitated the access

Auburn’s Statement: > “We want to state clearly: this access occurred unknowingly to us. The City of Auburn has not knowingly allowed, nor will we allow, direct access to our Flock system by U.S. [Border Patrol].”

Lakewood Police Chief Patrick Smith: > “Unbeknownst to the Lakewood Police Department, somehow the US Border Patrol got temporary access to a Flock account and used the national lookup tool to query a few vehicles.”

Legal Concerns

Washington State Law RCW 10.93.160: Washington State law prohibits the use of surveillance systems for civil immigration enforcement purposes.

Questions Raised: - Did federal access violate state law? - How many agencies unknowingly granted access? - What other federal agencies have accessed Washington surveillance data? - Can agencies effectively control who accesses their surveillance systems?

IMPLICATIONS FOR PUBLIC RECORDS REQUESTS

Why This Matters

1. **Legal Precedent Established:** The Skagit County ruling provides strong legal backing for public records requests seeking surveillance camera data.
2. **Privacy Arguments Are Insufficient:** Agencies can no longer simply deny requests by claiming privacy concerns when surveillance is broad and indiscriminate.

3. **Federal Access Must Be Disclosed:** Given the UW report findings, agencies must disclose which federal agencies have accessed their surveillance data.
4. **Audit Logs Are Crucial:** Network audit logs showing who searched the data and why are essential for accountability.
5. **“National Lookup” Settings Matter:** Whether agencies have inter-agency search features enabled is now a critical transparency question.

What You Can Request

Based on these developments, public records requests should include:

- ✓ **The surveillance data itself** (images, license plate reads, video footage)
- ✓ **Network audit logs** showing all searches conducted by any agency
- ✓ **Search reasons/purposes** documented by searching agencies
- ✓ **Records of federal agency access** (ICE, Border Patrol, FBI, DEA, HSI, etc.)
- ✓ **Settings for “National Lookup”** or similar features
- ✓ **Communications** regarding federal access or data sharing
- ✓ **Security audits** conducted after the UW report was published
- ✓ **Policies** on federal agency access

Responding to Denials

If an agency denies your request:

For Privacy-Based Denials: - Cite the Skagit County ruling: *Rodriguez v. City of Sedro Woolley* (Nov. 2024) - Quote the judge’s finding that “broad and indiscriminate” surveillance must be disclosed - Point out that the court specifically rejected privacy arguments

For Other Exemptions: - Request the specific RCW 42.56 exemption being claimed - Ask for a detailed explanation of how the exemption applies - Consider appealing to the department head - Contact ACLU of Washington or other advocacy organizations

For “We Don’t Have Records” Claims: - Reference the UW report showing that audit logs exist in Flock systems - Ask whether the agency has checked with the vendor (Flock, Ring, etc.) - Request records showing the agency’s search for responsive documents

BROADER CONTEXT AND CONCERNS

National Trends

The Washington State situation is part of a broader national pattern:

1. **Rapid ALPR Expansion:** Flock Safety has expanded to thousands of communities nationwide since 2017
2. **Federal Access Nationwide:** The UW report noted that the issue extends beyond Washington, with federal agencies accessing local surveillance data across the country
3. **Abortion Surveillance:** The Texas case involving searches for abortion seekers has raised alarms in states like Washington that protect reproductive rights

4. **California Violations:** CalMatters reported that California law enforcement violated state law more than 1,000 times by sharing ALPR data with federal agents
5. **Constitutional Challenges:** The Institute for Justice launched the “Plate Privacy Project” challenging warrantless ALPR surveillance nationwide

Civil Liberties Concerns

ACLU of Washington’s Position: - Lack of state regulation around how surveillance technology can be used - Insufficient controls on data storage and retention - No clear limits on who can access data - Risks to immigrant communities, abortion seekers, and other vulnerable populations

Key Quote from ACLU-WA: > “One of our major concerns with this technology is that currently no state regulation in place around how the technology can be used, how that data is stored, who it can be shared with, and that’s why we’re seeing a lot of these risks and harms taking place today.”

Surveillance State Concerns

The combination of: - Broad, indiscriminate data collection - Indefinite data retention - Inter-agency sharing without oversight - Federal access without local knowledge - Lack of warrant requirements

...creates what civil liberties advocates describe as a “mass surveillance infrastructure” that tracks the movements of ordinary citizens going about their daily lives.

TAKING ACTION

For Individuals

1. **File Public Records Requests:** Use the templates provided to request information from your local police department
2. **Attend City Council Meetings:** Ask questions about surveillance camera deployments and policies
3. **Contact Elected Officials:** Express concerns about surveillance technology and federal access
4. **Join Advocacy Groups:** Connect with ACLU-WA, Washington Coalition for Open Government, or local civil liberties organizations

For Communities

1. **Demand Transparency:** Require agencies to publicly disclose surveillance deployments before implementation
2. **Advocate for Regulations:** Push for state or local laws regulating surveillance technology use
3. **Require Audits:** Demand regular public audits of who accesses surveillance data
4. **Community Input:** Ensure community members have meaningful input before surveillance systems are deployed

For Journalists and Researchers

1. **Investigate Local Deployments:** File public records requests to understand surveillance in your area
 2. **Follow the Data:** Request audit logs to see how surveillance data is actually being used
 3. **Track Federal Access:** Monitor whether local agencies are aware of federal access to their systems
 4. **Report Findings:** Bring transparency to surveillance practices through reporting
-

LEGAL AND ADVOCACY RESOURCES

Washington State Resources

ACLU of Washington - Website: <https://www.aclu-wa.org/> - Focus: Privacy, civil liberties, surveillance technology - Services: Legal advocacy, public education, policy work

Washington Coalition for Open Government - Focus: Public records access, government transparency - Services: Advocacy, education, legal support

Attorney General's Public Records Office - Website: www.atg.wa.gov/public-records - Services: Guidance on RCW 42.56, dispute resolution

National Resources

Electronic Frontier Foundation (EFF) - Website: <https://www.eff.org/> - Focus: Digital privacy, surveillance technology - Resources: Atlas of Surveillance database

Institute for Justice - Plate Privacy Project - Website: <https://ij.org/plate-privacy/> - Focus: Constitutional challenges to ALPR surveillance - Services: Litigation support, advocacy

American Civil Liberties Union (National) - Focus: Fourth Amendment rights, surveillance oversight

Legal Assistance

If you encounter resistance to your public records request: 1. Document all communications with the agency 2. Keep copies of all requests and responses 3. Note exact dates of submissions and responses 4. Contact ACLU-WA or another legal advocacy organization 5. Consider filing a complaint with the Attorney General's office 6. Consult with an attorney about potential legal action

LOOKING FORWARD

Potential Next Steps

Legislative Action: - Washington State Legislature could pass regulations similar to Virginia and Illinois - Local jurisdictions could adopt surveillance technology ordinances - Stronger data sharing

restrictions could be enacted

Continued Litigation: - The Skagit County ruling may be appealed - Other jurisdictions may face similar lawsuits - Constitutional challenges may reach state or federal appellate courts

Technology Changes: - Flock and other vendors may modify access controls - Agencies may implement stronger oversight mechanisms - Alternative, less invasive technologies may emerge

Public Awareness: - Continued reporting on surveillance practices - Community organizing around surveillance issues - Increased public scrutiny of surveillance deployments

Why Your Request Matters

Every public records request: - Increases government transparency - Provides data for researchers and journalists - Holds agencies accountable - Helps protect civil liberties - Contributes to the public's understanding of surveillance practices

The Skagit County ruling and the UW report have opened a window into surveillance practices that were previously opaque. Your participation in seeking transparency helps keep that window open.

FREQUENTLY ASKED QUESTIONS

Q: Will my public records request put me on a watchlist? A: Public records requests are a constitutional right. Filing such requests is protected activity and should not result in retaliation.

Q: How long will it take to get a response? A: Agencies must respond within 5 business days, though they may need additional time to fulfill complex requests.

Q: Will I have to pay for the records? A: Agencies may charge for copying costs, but many will provide electronic records at little to no cost. You can request a fee waiver.

Q: What if the agency says they don't have the records? A: Ask them to document their search for records. Given the UW report findings, audit logs should exist if they use Flock or similar systems.

Q: Can I request data that includes my own vehicle? A: Yes, and you may have additional rights under privacy law to access data specifically about yourself.

Q: What if the agency cites an exemption? A: They must cite a specific RCW 42.56 exemption and explain how it applies. You can appeal if you believe the exemption is being misapplied.

CONCLUSION

The November 2024 Skagit County Superior Court ruling represents a significant victory for government transparency in Washington State. Combined with the revelations in the UW Center for Human Rights report, these developments have created both an opportunity and an obligation for citizens to demand accountability regarding surveillance technology.

Your public records requests are not just about obtaining information — they're about ensuring that government surveillance programs operate with transparency, oversight, and respect for civil liberties.

The precedent is clear: Surveillance data is public data. The question now is whether agencies will embrace transparency or continue to resist it.

This document is for informational purposes only and does not constitute legal advice. For specific legal guidance, consult with an attorney.

Document Version: 1.0

Last Updated: November 2024

Sources: Skagit County Superior Court records, UW Center for Human Rights, news reports, public agency statements