

BEND
PRIVACY ALLIANCE

*Watching the
watchers since 2026*

Surveillance in Our Community

A community conversation on what local technology collects,
who has access, and why oversight matters —
held during the ALPR National Week of Action.



Wednesday, August 19



5:00–7:00 PM



Central Library,
61956 SE Santorini St,
Bend, OR 97702



Bend Privacy Alliance





Our purpose

Bend Privacy Alliance is a nonpartisan community group working to protect privacy, promote transparency, and ensure local technology is accountable to the people.



*We believe a safer community
is a community that respects
privacy and civil rights.*



Protect privacy

Question how data is
collected, used, stored,
and shared.



Promote transparency

Seek clear policies,
public records, and
open decision-making.



Ensure accountability

Advocate for oversight,
limits, and measurable
safeguards.



Empower community

Share information,
build civic power, and
support each other.



Better questions. Better policies. Better Bend.



Our principles

These principles guide how we evaluate technology, policy, and public decisions that affect our community.



Privacy by default

Protect personal data and limit collection to what is necessary and lawful.



Transparency first

The public has the right to know what technology is used and how it works.



Accountability and oversight

Strong policies, auditing, and independent oversight are essential.



Community centered

Residents deserve a real voice in decisions that impact their lives.



Proportional and necessary

Tools should be effective, proportionate, and the least intrusive option.



Our rights. Our data. Our community.



Why it matters

Surveillance decisions made today shape our freedom, our safety, and our community for years to come.



Technology can help our community—when it is used with limits, oversight, and public input.



◆ Our choices today determine the kind of community we build tomorrow. ◆



Protect civil rights

Unchecked surveillance can chill free speech, movement, assembly, and association.



Build public trust

Transparency and oversight help ensure technology is used fairly and responsibly.



Invest in what works

Focus resources on real community needs—not technology for its own sake.



What we'll cover together

Tonight's conversation will cover how ALPR and connected technologies work, what's happening in Bend, the legal and policy context, and what we can do as a community.



1. How ALPR works

How license plate readers capture data and turn it into a searchable record.



2. What's happening in Bend

Current and proposed systems, policies, and public records.



3. Legal and policy context

Oregon laws, court rulings, and policy frameworks that matter.



4. Vendor systems and data flows

How data moves through platforms, databases, and other agencies.



5. Risks and harms

Privacy, civil rights, security, and equity concerns we should understand.



6. What we can do together

Practical actions, public engagement, and next steps as a community.



This is your community. Your questions and experiences matter.



Our conversation guidelines

A few simple guidelines help us create a space where everyone feels safe, respected, and empowered to participate.



Be respectful

Treat everyone with kindness. Disagree without being disagreeable.



Listen actively

Give others your full attention. Listen to understand, not to respond.



Share airtime

Be mindful of time so more voices can be heard.



Share safely

Avoid personal attacks. Keep stories and data as accurate and verifiable as possible.



Focus on solutions

Let's be curious, collaborative, and action oriented.



These guidelines help us build trust and do our best work—together.



What is an ALPR?

An Automated License Plate Reader (ALPR) uses cameras and software to read license plates and turn them into data.



1. Camera

A camera captures images of vehicles as they pass.



2. Plate read

Software reads the characters on the license plate.



3. Data record

The plate, time, location, and image are recorded.



4. Searchable

The plate can be searched and shared.



Plate number

The license plate characters captured.



Date and time

When the observation was made.



Location

Where the observation took place.



Image or attributes

A photo or details such as make, model, color, and body style.



Every read creates a data point. Every data point has the potential to be used.

Two forms of ALPR

Stationary

◆ proposed or debated in Bend

Mounted at a fixed location

Continuously watches the same
roadway or entrance



Plate number

The license plate
characters captured.



Vehicle image or attributes

A photo or details like
make, model, color,
and body style.



Date and time

When the observation
was made.



Location

Where the observation
took place.

Mobile

◆ documented in Bend fleet systems

Mounted on a patrol
or parking vehicle

Collects observations
wherever the
vehicle travels



Plate number

The license plate
characters captured.



Vehicle image or attributes

A photo or details like
make, model, color,
and body style.



Date and time

When the observation
was made.



Location

Where the observation
took place.



◆ Bend's documented surveillance discussion includes both forms. ◆



How ALPR is used

The data ALPR systems collect can be used for a variety of purposes—some routine, some high-impact.

Common use cases include:



Investigations

Find vehicles connected to a crime or persons of interest.



Stolen or wanted vehicles

Identify stolen cars or vehicles linked to warrants.



Traffic and parking enforcement

Support parking rules, tolling, and traffic management.



Public safety alerts

Receive alerts for hot lists, AMBER Alerts, or missing persons.



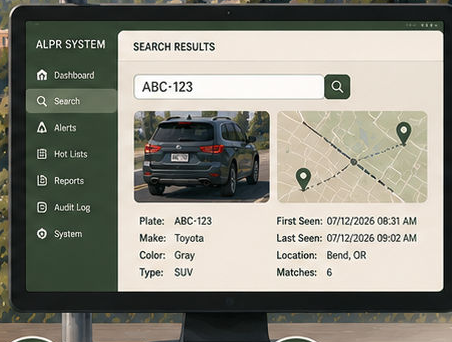
Administrative uses

Support audits, reporting, fleet management, and agency operations.



Other agency requests

Share or respond to data requests from other local, state, or federal agencies.



Use depends on policy. Oversight ensures the technology serves the public—responsibly.

What ALPR systems can capture

 OVERVIEW

ALPR systems create detailed records every time a vehicle is seen. Individually, each record may seem small. Together, they reveal more than we might expect.



License plate number

The plate is the most direct identifier and the starting point for all other data.



Date, time, and location

Records show when and where a vehicle was seen, building a timeline of movements.



Vehicle attributes

Make, model, color, type, and other details help identify the vehicle beyond the plate.



Images

Photos of the plate and often the full vehicle provide visual context.



Direction of travel

Shows which way the vehicle was moving at the time of capture.



Confidence score and reads

Indicates how confident the system was and may include multiple reads of the same vehicle.



Additional context

May include camera ID, weather, speed, or nearby events, depending on system settings.



◆ *Data points connect. Patterns emerge. Privacy shrinks.* ◆

BEND
PRIVACY ALLIANCE

*Watching the
watchers since 2026*



PRIVACY IMPACT IS CUMULATIVE

One observation versus a pattern

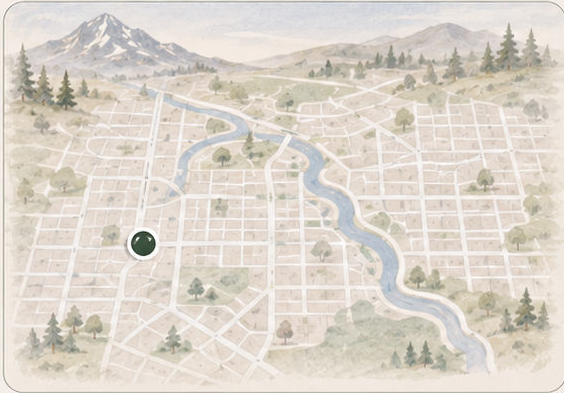


ILLUSTRATION

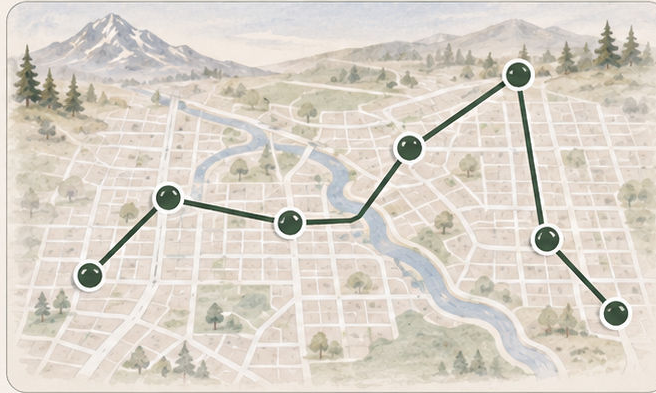
One observation is a vehicle at a place and time.

Repeated observations can reveal a routine.

..... ♦ one observation ♦



..... ♦ a pattern ♦



Home



Work



School drop-off



Clinic



Place of worship



Recovery meeting



Protest or public meeting



..... ♦ A hypothetical illustration of how location data becomes more sensitive as observations accumulate. ♦

BEND
PRIVACY ALLIANCE

*Watching the
watchers since 2026*



VERIFIED LOCALLY / PROPOSED



A camera is only the first step



1. Camera



2. Vendor or
agency platform



3. Search and
alert functions



4. Other authorized
users or systems

Questions begin after collection:



Where is
it stored?



How long is
it kept?



Who can
search it?



What sharing
is enabled?



Are searches
logged and audited?



Where ALPR data can go

A single plate read can travel far beyond the moment and place it was captured.

From one read to many uses:



Captured

A camera reads a license plate as a vehicle passes by.



Stored

The data is uploaded to a system and digitally stored.



Connected

It can be combined with other datasets and systems.



Searched

Authorized users query the data for investigations or other purposes.



Shared

It can be shared with other agencies or outside organizations.



Used

The information can influence decisions about people and communities.



1. CAPTURE

A plate is read by an ALPR camera.



2. STORE

The read is time-stamped, geotagged, and stored in a database.



3. CONNECT

The data can be linked with other systems and information.



4. SEARCH

Authorized users can search the data for matching plates or patterns.



5. SHARE

Data can be shared with other agencies or private partners.



6. USE

The data can be used for enforcement, investigations, or other decisions.



DATA JOURNEY

Where it can go



Local law enforcement and city departments



State and federal agencies



Regional law enforcement databases



Private companies and vendor systems



Insurance companies and data brokers



Analytics, AI tools, and predictive systems



Bend Privacy Alliance



Transparency. Accountability. Community.



OUR DATA. OUR RIGHTS. OUR CHOICES.

One read. Many connections.

ALPR data rarely stays in one place.
It connects to many systems and many purposes.

That means it can be:



Searched

Across agencies and systems.



Matched

With other data about people, vehicles, and locations.



Analyzed

To find patterns, predict behavior, or assess risk.



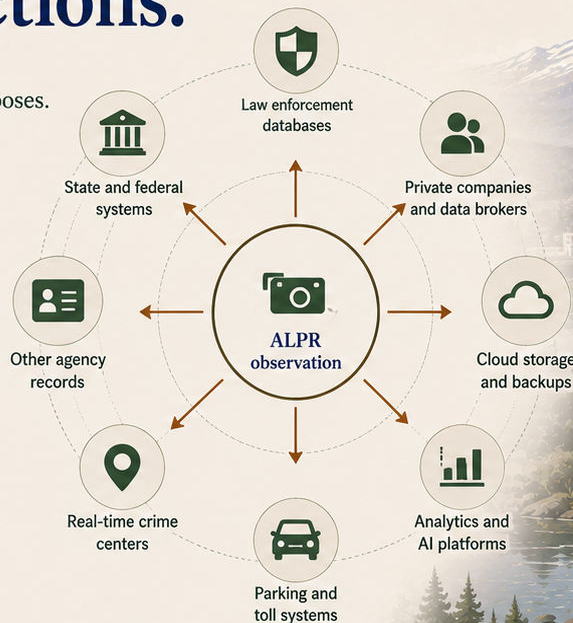
Shared

With government agencies, vendors, and private partners.



Stored

For months or years in multiple databases.



THE NETWORK EFFECT

Examples of connected data



People

DMV records, voter rolls, watchlists, and other identity data.



Vehicles

Registration, ownership, insurance, and inspection data.



Places

Home addresses, workplaces, places of worship, clinics, and protests.



Time

Patterns of movement over days, months, and years.



Events

Traffic stops, warrants, investigations, and incident reports.



The more connections, the greater the impact on our rights and freedoms.



Bend Privacy Alliance

◆ Transparency. Accountability. Community.



INFORMED TODAY. PROTECTED TOMORROW.

What AI processing adds on top of plate reads

Modern ALPR systems do more than read characters from a plate. AI layers add description-based search, relationship inference, time depth, and fusion with other data systems.

AI + ANALYTICS LAYER

Four new layers of analysis



1. Vehicle fingerprinting

Some systems build a searchable vehicle fingerprint: make, model, body style, color, decals, bumper stickers, roof racks, damage, and other visual features.

- ◆ A vehicle can still be tracked when the plate is obscured, swapped, stolen, or misread.



2. Convoy / association analysis

Vehicles that repeatedly appear near each other across time and place can be flagged as a convoy or association pattern.

- ◆ That turns proximity into an inference about relationships, routines, or networks.



3. Historical retention

Retention turns isolated scans into a pattern-of-life record. Repeated sightings can reveal home, work, worship, medical visits, recovery meetings, protests, or a partner's address.

- ◆ It also enables retroactive searches once someone becomes interesting to investigators.



4. Fusion with other systems

ALPR data can be fused with facial biometrics, surveillance footage, social media, and commercial location data.

- ◆ Vehicle seen at location X can become identified person seen at location X.



1. Plate read

One scan of one vehicle



2. AI vehicle fingerprint

Description-based search even without a plate

"Gray Honda CR-V · roof rack · dented rear bumper"



3. Association + retention

Who travels together — and where over time



4. Fusion

Cross-linked with other data systems



Why reform focuses here



30-day retention caps limit time depth



Warrants for historical queries limit retroactive tracking



Audit logging of every search helps detect misuse

Reducing any one of these variables meaningfully limits what the whole system can reveal.



◆ Plate read + AI inference + retention + data fusion can reveal far more than a single moment on the road. ◆

Sources referenced: BPA Link Archive entries on vehicle fingerprinting and convoy analysis; ICE RAVEn reporting; Carpenter line of reasoning.



Bend Privacy Alliance

◆ Transparency. Accountability. Community.



TODAY'S DECISIONS SHAPE TOMORROW'S REALITY.

Bend's ALPR story

How procurement, configuration, public records, and public pressure shaped the debate

 Completed / Documented

 Pending / Contested



2022

Council approves
Axon fleet-camera
procurement



2023–2026

Mobile ALPR use is
later documented in
Bend's fleet environment



2025

Flock stationary
cameras enter the
local debate



January 2026

Flock cameras
are turned off



May–July 2026

Axon stationary ALPR,
Policy 428, and public
oversight become
active issues



August 2026

Public decisions and
policy questions
remain



BEND
PRIVACY ALLIANCE

*Watching the
watchers since 2026*



VERIFIED WITH QUALIFICATION

License plate readers are already operating from Bend police vehicles.

The public record shows Council approved
the broader fleet-camera procurement.



What remains less clear is whether ALPR
activation was separately presented and
authorized as its own policy decision.



Bend's surveillance environment is an ecosystem

CONNECTION LEGEND

- Documented relationship
- - - Possible integration or vendor-supported capability

STATUS LEGEND

- Confirmed active or contracted
- Proposed, pending, or activation withheld
- Vendor or integration capability
- Unknown configuration or records needed



SOFTWARE CURRENTLY USED BY BEND POLICE DEPARTMENT

These tools support policing, investigations, records, communications, and public information in our community.



TRANSPARENCY.
ACCOUNTABILITY.
COMMUNITY.



EVIDENCE & BODY-CAMERA ECOSYSTEM (AXON)



Axon Evidence (Evidence.com)
Cloud evidence management.



Axon Evidence Sync
Automated evidence upload and sync.



Axon Evidence Upload XT
Upload tool for large evidence files.



Axon View
Mobile app to review evidence.



Axon Capture
Smartphone video recording app.



Axon - Respond Plus
Real-time location and response updates.



Axon - Standards
Use-of-force and incident tracking.



RECORDS, REPORTING & CASE MANAGEMENT



**Administrative Investigations
Management (AIM) Web**
Internal affairs and admin investigations.



eSoph
Background investigations.



Oregon State ONIBRS
Oregon Incident-Based Reporting System.



LEDS 20/20
Law Enforcement Data System
client application.



CrimeView Dashboard
Crime analysis and mapping.



JustFOIA
Public records request software.
(Also used by City Manager's Office)



DISPATCH / FIELD TOOLS



Live911
Lets officers listen to 911 calls directly.



Tyler ShieldForce
Mobile and tablet field application.



SPIDR Tech
Automated public-notification and
engagement platform.



RADIO & DEVICE MANAGEMENT



Motorola APX CPS
Radio programming software.



Lock n Charge
Laptop checkout and
charging system.



Data Collection tools.
3rd party vendors. ♦
Where's the oversight?



FORENSIC & CRASH INVESTIGATION



Bosch CDR Software
Crash Data Retrieval (vehicle "black box" export).



TruView (Leica Geosystems)
Collision forensic scene mapping.



Datacolor Spyder5 Pro
Monitor color calibration for forensic imaging.



DRONE / MAPPING



Pix4D
Drone mapping and
image stitching.



GENERAL OFFICE / ADMIN TOOLS ALSO ASSIGNED TO POLICE



Sign-Up Genius



Smarts - Text Message Archival
(Verizon Wireless integration)



Garmin Express



Paperport Image Printer



Visio Data Visualizer



Embrava Blynclight
(Also used by Finance)



MSDOnline
(Also used by Utility)



BEND PRIVACY ALLIANCE

♦ Watching the watchers since 2026.



TOOLS ARE ONLY AS POWERFUL AS THE POLICIES THAT GUIDE THEM.

Retail Surveillance: Inside the Black Box

Retail stores use cameras and sensors that quietly collect, analyze, and share data about everyone who walks in. It doesn't stop at shoplifting—these systems track you, profile you, and influence what you see, pay, and do.



Retail surveillance is not just about theft prevention. It's a data-driven business model.

THE RETAIL SURVEILLANCE PIPELINE



1. COLLECT

Cameras, sensors, and apps capture data about you and your devices.



2. IDENTIFY

AI systems recognize faces, bodies, devices, and behaviors.



3. ANALYZE

Data is turned into insights about movement, habits, dwell time, and purchases.



4. PROFILE

Profiles reveal interests, income level, loyalty, and risk.



5. MONETIZE

Data drives ads, dynamic pricing, loss prevention, and third-party sales.



BEYOND THE PUBLIC EYE



CAMERAS & SENSORS

Record video, audio, Wi-Fi, and device signals.



IDENTIFICATION

AI detects faces, license plates, and behaviors.



DATA ANALYSIS

Tracks movements, counts visits, builds behavioral profiles.



SHARING & USE

Data is shared with vendors and used for advertising, pricing, and more.



◆ You are more than a shopper. You are data. ◆

How ALPR systems have been abused

Patterns documented in reporting, litigation, audits, and BPA's Link Archive.

 DOCUMENTED MISUSE

Common abuse patterns



Personal stalking by officers

At least 21 confirmed cases appear in the Institute for Justice tracker. Flock's chief legal officer has called ex-partner tracking the most common form of misuse.



Georgia cluster (July 2026)

Five cases surfaced within days: former Albany officers, a Greene County deputy, and three Cherokee County deputies. In Cherokee County, the misuse count tripled once someone audited the logs.



Vendor-side misuse

A Flock vice president reportedly viewed footage 185 times, including footage from inside a children's gymnastics room, apparently for sales-pitch purposes.



Audit-log gaming

Law360 reported that many searches used vague or meaningless justifications, including extremely short search reasons and entries like "la la la la la."



Retaliation against critics

Kansas Watch flagged a Lenexa police chief who allegedly used ALPR to help orchestrate a pretextual stop against a resident who wrote a critical op-ed.



Disparities and adjacent database misuse

A Norfolk study found much denser camera placement in majority-Black tracts. Comparable database failures include CalGang errors and Phoenix's reported gang-database targeting of protesters.



21+

confirmed
stalking cases



5

Georgia cases
surfaced within days



185

reported vendor-side
footage views



13.5%

of 184.2M searches
had reasons of 3
characters or fewer
*Nearly 2 million used
a single-character reason.*

What these cases show



Misuse is often personal, retaliatory, or hidden inside routine systems.



Abuse expands when logs are not independently reviewed.



The recurring reforms across sources are warrants and mandatory independent audits.



Reactive self-policing rarely catches abuse until someone is forced to look.

Sources: Institute for Justice tracker; IPVIM; Law360; Kansas Watch; Voice of OC; Brennan Center. Compiled from BPA Link Archive.



Bend Privacy Alliance

◆ Transparency. Accountability. Community.



OUR COMMUNITY. OUR DECISIONS. OUR FUTURE.

State law, sanctuary law, and the data-sharing dispute

How Oregon's ALPR reforms, local shutdowns, and a separate OSP records-access lawsuit fit together.



STATE LAW + PENDING LAWSUIT

What SB 1516 did



Limits ALPR use to defined law-enforcement purposes



Requires deletion after 30 days unless tied to an active investigation



Restricts uses that would violate Oregon's sanctuary law



Requires search logging



EFF and ACLU of Oregon said the law still leaves loopholes.

Stronger examples cited



Washington: limits ALPR near schools, health sites, and religious sites; bars tracking abortion or gender-care seekers and protesters



Texas: requires a warrant



5

Oregon cities turned off Flock cameras



279

federal immigration queries into Bend's Flock data



1.4M

LEDs / NLETS queries alleged in the pending OSP lawsuit



170K+

ICE queries alleged in that lawsuit

Why local shutdowns happened



Bend, Albany, Eugene, Springfield, and Woodburn turned off Flock cameras



Woodburn did so after confirming immigration enforcement had accessed city camera data dozens of times



In Bend, reporting documented 279 federal immigration queries into the city's Flock data



The shutdowns helped drive the debate around SB 1516

Keep the systems separate



ALPR / Flock data



- License-plate camera scans
- Vehicle sightings by place and time
- Bend-specific reporting focused on this system
- These concerns helped push local shutdowns



LEDs / NLETS records access



- Driver records, vehicle registrations, and other law-enforcement records
- Operated in Oregon through OSP's systems
- Pending Rural Organizing Project lawsuit concerns this system
- This is not the same as a license-plate camera scan database



Key distinction: the pending OSP lawsuit is about LEDs / NLETS records access — not the same database as local Flock ALPR camera scans.

Sources referenced: Willamette Week; Oregon Capital Chronicle; The Source Weekly; Atlas of Surveillance; KGW. Distinguish verified reporting from lawsuit allegations.



Bend Privacy Alliance

Transparency. Accountability. Community.



OUR COMMUNITY. OUR DECISIONS. OUR FUTURE.

Other surveillance tools to know

ALPR is only one part of a much larger surveillance ecosystem. These categories are used by agencies around the country.

 SURVEILLANCE TECHNOLOGY TYPES



Common categories

- | | |
|--|--|
|  1. Facial recognition
Matches faces from photos or video against image databases. |  7. Fusion centers
Regional information-sharing hubs linking agencies and intelligence sources. |
|  2. Body-worn and fleet cameras
Record encounters, traffic stops, and patrol activity. |  8. Data brokers and risk platforms
Systems that buy, combine, or score personal and commercial data. |
|  3. Municipal and cloud camera systems
Networked fixed cameras in streets, buildings, or public facilities. |  9. OSINT / social media surveillance
Tools that monitor public posts, networks, and online activity. |
|  4. Audio and gunshot detection
Microphones and software that claim to detect gunfire or other sounds. |  10. Predictive policing and gang databases
Systems that flag people, places, or groups for added scrutiny. |
|  5. Drones / UAS
Aerial cameras used for search, monitoring, mapping, or tactical response. |  11. Retail surveillance and camera sharing
Store cameras, loss-prevention systems, and police access partnerships. |
|  6. Real-time crime centers
Platforms that pull together live feeds, alerts, and police data. |  12. AI police report writing and analytics
Software that drafts reports or generates inferences from collected data. |

What many of these tools do



Collect

Capture images, audio, location, or other personal data.



Identify

Match a person, vehicle, device, or account.



Track

Follow movements, routines, or associations over time.



Share and combine

Move data across agencies, vendors, or platforms.

A good public question



Before any technology is adopted, the public should ask what it collects, how long it is kept, who can search it, and who approved it.

◆ *Different tools use different sensors — but the same accountability questions still apply.* ◆



Bend Privacy Alliance

◆ Transparency. Accountability. Community.



OUR COMMUNITY. OUR DECISIONS. OUR FUTURE.

How AI data centers connect to surveillance architecture

The buildings that power AI systems also store surveillance data and shape how those systems expand.

1. Compute makes AI surveillance possible



AI vehicle fingerprinting, facial recognition, convoy analysis, predictive policing, and AI report writing all rely on physical data centers, chips, and electricity. These tools are not abstract software alone — they run on real infrastructure.



Every inference call happens on a physical server somewhere.

2. Surveillance data is physically warehoused



Surveillance records do not just 'live in the cloud.' They are stored in real buildings, under specific ownership and legal jurisdictions.



Where the building is located can shape what rules apply.

Reported example:

Microsoft was reported to have hosted roughly 11,500 TB of intercepted Palestinian phone-call data — about 200 million hours of audio — in European data centers.



Data centers



Train / run
AI models



Store and fuse
surveillance data



Secure infrastructure /
monitor opposition

3. The feedback loop



The same fusion-center style architecture used to watch communities has also been used to monitor people organizing against AI data centers. Reporting on the Delaware Valley Intelligence Center described anti-data-center organizing being framed as a security concern despite no identified attack plan.



Protected speech can be recharacterized as a threat.

4. Vendor and systems convergence



The same ecosystem of companies, investors, and agencies appears across data centers, AI analytics, and large-scale surveillance fusion. Platforms can combine records from cameras, biometrics, government databases, and other sensors into one operational picture.



Examples discussed in BPA materials include Palantir- and Anduril-linked fusion models.

Why this matters



Data centers are not a separate issue sitting next to surveillance technology. They are part of the same architecture: they power the tools, hold the data, and can become a target for the same surveillance logic used against communities.



Physical infrastructure + stored data + AI analytics = surveillance capacity

Sources referenced in BPA materials: BPA Substack primer; Guardian / 972mag / Microsoft reporting; DVIC reporting; Restore the Fourth; Mijente / Prism reporting.



Data doesn't stay local



ALPR data can leave Bend through formal requests, system connections, and vendor sharing.

Common ways data leaves our community:



Law enforcement requests

Requests from local, state, tribal, and federal agencies.



System integrations

Connections to regional databases, fusion centers, and national networks.



Vendor sharing and partnerships

Private companies may share data with other vendors or data brokers.



Third-party data sales

Some vendors allow data to be sold or licensed to outside organizations.



Retention and future use

Data stored today can be accessed, shared, or used in ways we can't predict tomorrow.

Where ALPR data can go



Local systems

Bend PD databases and records.



Regional sharing

Regional databases, fusion centers, and task forces.



National databases

NCIC, federal systems, and national networks.



Other agencies

Police departments, sheriff's offices, and state agencies across the country.



Private sector

Vendors, data brokers, insurers, and other commercial uses.



Once data leaves our community, we lose control over how it's used, shared, and protected.



Bend Privacy Alliance

◆ Transparency. Accountability. Community.



OUR DATA. OUR RIGHTS. OUR CHOICES.

Vendors are part of the story

ALPR systems are built, operated, and improved by private companies. Their choices affect our privacy, our security, and our rights.

 THE VENDOR LAYER

What vendors provide



Hardware

Cameras, readers, mounts, and sensors.



Software platforms

Capture, storage, search, and analytics.



Cloud infrastructure

Servers, backups, and system uptime.



AI and analytics

Tools that turn data into insights.



Customer support

Training, help desks, and system management.



Product updates

New features, changes, and default settings.



Security practices

Encryption, access, controls, and monitoring.



Data policies

Retention, sharing, and use limitations.



Strong oversight includes asking hard questions about vendors—not just the technology.

Why vendor choices matter



Vendor access

Vendors may access data for support, maintenance, training, or product improvement.



Data sharing

Some vendors share data with other companies or partners, often in ways we can't fully see.



Data stored outside our control

Information may be stored outside Oregon or the U.S., subject to different laws and protections.



Changing terms and features

Policies, settings, and features can change—sometimes without public notice.



Security and breach risk

Vendors are targets for hackers, and breaches can expose our community's data.



Transparency starts with knowing who has the data, what they can do with it, and how they are held accountable.



Bend Privacy Alliance

◆ Transparency. Accountability. Community.



OUR DATA. OUR RIGHTS. OUR CHOICES.

Purposes can expand

What begins as a narrow purpose can grow.
Today's use can become tomorrow's routine.

Purpose creep warning signs:



Function creep

Systems built for one use are gradually used for more.



Policy drift

Policies and rules change quietly, often without public notice.



Mission expansion

Agencies request more access and broader permissions over time.



Normalization

Surveillance becomes routine, accepted, and hard to roll back.



Irreversibility

Data collected today can persist for years or decades.

Common secondary uses



Investigations

Using ALPR data for investigations beyond the original reason it was collected.



Immigration enforcement

Sharing data with federal agencies for immigration-related purposes.



Analytics and profiling

Analyzing movement patterns to predict behavior or build dossiers.



Marketing and advertising

Using movement data to target ads or influence consumer behavior.



Civil actions and collections

Sharing data with private parties for parking, tolls, debt collection, or litigation.



Other future uses

New technology and new agreements create new possibilities.



PURPOSE EXPANSION



Once collected and shared, ALPR data can be used in ways the public never anticipated and can be very difficult to undo.



Bend Privacy Alliance

◆ Transparency. Accountability. Community.



TODAY'S DECISIONS SHAPE TOMORROW'S REALITY.



What's at risk in Bend and Central Oregon?



Your privacy — Personal information, movements, and daily life are collected, stored, and shared — often without your knowledge.



Your civil rights — Mass surveillance and data sharing can chill free speech, assembly, and community participation.



Your community values — Trust, transparency, and accountability are essential to a healthy, free and fair society.



Your future — Technology choices made today shape the rights, opportunities, and quality of life for generations to come.

WHY IT MATTERS



Transparency builds trust.

Clear rules and oversight keep our community strong.



Accountability protects everyone.

Checks and balances prevent abuse of power.



Smart policy keeps us safe.

Good governance ensures technology serves the people — not the other way around.



A private community is a resilient community.

Protecting our data today preserves our freedom tomorrow.



Privacy. Transparency. Civil Rights.

LET'S WORK TOGETHER FOR A MORE PRIVATE, STRONGER BEND.

Learn more. Get involved. Make your voice count.

Oversight makes the difference

Strong rules and transparency turn powerful technology into a tool that serves public safety—without sacrificing our rights.



SOLUTIONS

Why oversight is needed:



Prevent overreach

Clear rules keep monitoring focused on legitimate public safety needs.



Limit retention

Keep data only as long as necessary and delete what isn't.



Ensure accountability

Logs, audits, and transparency create checks and balances.



Protect privacy

Minimize what is collected, secure what is kept, and restrict who can access it.



Build public trust

Open policies and community input make our city safer and stronger together.

What strong ALPR oversight looks like



Clear policies

Define lawful uses, prohibit misuse, and set strict data retention limits.



Access controls

Limit access to trained personnel with a documented need to know.



Transparency and logs

Maintain detailed logs and publish regular transparency reports.



Independent audits

Regular third-party audits ensure compliance and effectiveness.



Community oversight

Community review and input keep policies aligned with our values.



Oversight doesn't slow down public safety—it keeps it focused, fair, and effective.

Key oversight questions



What data do we collect and why?



How long is the data kept and why?



Who has access and under what rules?



How are searches logged and reviewed?



How do we ensure data security?



How can the public see and shape policy?



BEND
PRIVACY ALLIANCE

Watching the
watchers since 2026

Good rules today protect our rights tomorrow.



OUR COMMUNITY, OUR STANDARDS

The legal context in Oregon



LEGAL CONTEXT

Oregon has laws that protect our data and limit government overreach.
Here are key laws and principles that apply to ALPR use.

State privacy laws



Oregon Consumer Privacy Act (OCPA) (ORS 646A.600–646A.638)

- ◆ You have the right to know what personal data is collected.
- ◆ You can access, correct, and delete your personal data.
- ◆ Sale of personal data of minors under 16 is prohibited.
- ◆ Government entities are subject to these requirements.



ALPR data tied to individuals is personal data.

Public records access



Oregon Public Records Law (ORS 192.311–192.478)

- ◆ We have the right to request and obtain public records.
- ◆ ALPR policies, data use, and audit logs can be public records.
- ◆ Fees can be waived if disclosure is in the public interest.
- ◆ Agencies must respond in a reasonable time.



Transparency is our right. Use it.

Limits on surveillance



Constitutional & Oregon protections U.S. & OR Constitutions

- ◆ We are protected from unreasonable searches and seizures.
- ◆ Mass surveillance without suspicion raises serious constitutional concerns.
- ◆ Data collected for one purpose should not be used for another without legal authority.



Our rights were designed before this technology. We must defend them now.

Recent ALPR law



SB 1516 (2026) Oregon ALPR Act *Effective March 31, 2026*

- ◆ Sets statewide minimum standards for ALPR use by law enforcement.
- ◆ Requires policies, transparency, data limits, and audit requirements.
- ◆ Does not override stronger local protections—local control matters.



State law sets the floor. Our community can set the standard.



These laws give us tools. Community oversight ensures they are honored.

BEND
PRIVACY ALLIANCE

*Watching the
watchers since 2026*



KNOW THE LAW. USE YOUR RIGHTS.

Oregon's 30-day rule

Oregon SB 1516 generally limits ALPR retention to no more than 30 days. Exceptions apply in specific circumstances.

What SB 1516 establishes


30 days
general maximum
retention period



Exceptions apply
when data relates to:

- ◆ An ongoing criminal investigation
- ◆ A court proceeding

The law also addresses:



authorized uses



federal and
out-of-state access



audits



contracts



encryption
requirements



civil
remedies



◆ *State law sets a floor—but public oversight still matters.* ◆



Retention varies and policies matter

ALPR data can be stored from days to years depending on the system and local policy. Shorter retention reduces risk.

What influences retention?



System settings

Vendors offer different defaults and options that agencies can configure.



Policy choices

Agencies decide how long to keep data, for what purposes, and under what rules.



Legal requirements

State and federal laws may require minimum retention for specific investigations or cases.



Operational needs

Legitimate needs should be balanced with privacy and security responsibilities.



What should Bend's ALPR retention policy look like? (Time limits • Purposes • Exceptions • Oversight)



Retention varies—policies matter

Some systems keep data automatically



Even without a specific look-up, ALPR systems may store data for set periods based on system defaults or vendor configurations.

Data may be retained for:



Active investigations

To support ongoing cases and identify suspects or patterns.



Court and legal requirements

To meet discovery obligations or court orders.



Administrative purposes

To manage operations, audit use, or ensure compliance.



After retention ends

Data should be securely deleted or permanently anonymized.

Why clear retention rules matter



Limits risk

Less data stored means less chance of misuse, breach, or error.



Respects rights

Protects privacy and reduces the potential for chilling effects.



Builds trust

Clear limits and transparency help the public have confidence in the system.



Supports accountability

Defined retention periods make oversight, auditing, and reporting possible.

Policy choices shape the outcome

Technology is just a tool.
Our policies decide how it's used—and how it affects us.

Key policy decisions include:



Retention limits

How long is data kept—and why?



Access and oversight

Who can access data, and how is it audited?



Purpose limitations

What are the approved uses—and what's prohibited?



Transparency and reporting

What the public can see, and how often.



Security and safeguards

How data is protected from misuse and breaches.

Questions we should be able to answer:



How long is
ALPR data
retained?



Who can access
the data—and
under what
conditions?



What laws and
policies govern
its use?



What is
prohibited
and why?



How is the
public informed
and included?



What steps
protect our
rights and
privacy?



We get to decide what kind of Bend we want to live in.



Bend Privacy Alliance

◆ *Transparency. Accountability. Community.*



OUR DATA. OUR RIGHTS. OUR CHOICES.

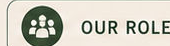


POLICY MATTERS



Who decides what is acceptable?

Surveillance decisions shape our community.
We all have a role in setting the rules.



Decision-makers and influencers



Elected leaders

City Council, County Commission, and other elected officials set policy, approve budgets, and shape priorities.



Law enforcement

Agencies choose how technology is used day to day and what data is collected, queried, and shared.



Community members

Residents bring values, lived experience, and expectations that should guide surveillance decisions.



Advocates and organizations

Local groups and partners raise awareness, share expertise, and advocate for strong protections.



Vendors and contractors

Technology providers build systems and set features, default settings, and business practices.



Oversight bodies

Auditors, courts, inspectors general, and watchdogs help ensure accountability and legal compliance.



Democratic oversight, transparency, and strong policies help ensure technology serves our community—not the other way around.

Questions we should be asking



What problem are we trying to solve?



Are the benefits worth the risks to our rights and our community?



How will this be used, monitored, and limited?



How will our data be protected and our rights respected?



Who will be affected—and who gets to have a say?



How will we know if it's working as promised?



Bend Privacy Alliance

◆ Transparency. Accountability. Community.



OUR COMMUNITY. OUR DECISIONS. OUR FUTURE.

Principles for responsible surveillance in Bend

Strong principles help ensure surveillance technology protects our community and our rights.



Necessity

Use surveillance only when it is necessary to address a clearly defined public safety need.



Proportionality

Match the scope, duration, and data collected to the specific need—no more.



Transparency

Be open about what technology we use, why, and how it works.



Accountability

Ensure oversight, logging, audits, and consequences for misuse.



Privacy and civil rights

Protect privacy, prevent discrimination, and respect every person's rights and dignity.

Putting principles into practice



Define the need

Clearly explain the problem and why surveillance is the right tool.



Set limits

Limit what we collect, how long we keep it, and how it can be used or shared.



Protect the data

Use strong security, minimize access, and guard against breaches.



Provide oversight

Require logs, audits, public reporting, and independent review.



Engage the public

Invite community input and revise policies as needs and values evolve.



◆ *Good policies today can prevent harms tomorrow.* ◆



Bend Privacy Alliance

◆ *Transparency. Accountability. Community.*



TOGETHER, WE SET THE STANDARD.

The ask

A clear rule for surveillance decisions in Bend.



THE ASK

Bend should require public notice,
a public record, and accountable rules
before a new surveillance
capability is activated.



Those same rules should govern
what is already operating.



Good governance begins before activation.



Public notice

Tell the community
what is being
proposed.



Public record

Document the
decision, scope,
and rationale.



Accountable rules

Set clear limits,
audits, and
oversight.



Bend Privacy Alliance

◆ Transparency. Accountability. Community.



PUBLIC NOTICE. PUBLIC RECORD. ACCOUNTABLE RULES.

What you can do to make a difference

Informed, engaged communities build safer, more just, and more free places to live.



“When we show up, ask questions, and demand accountability, our voices shape the rules that govern our future.”

Ways to take action



Learn and stay informed

Understand the technology, follow local decisions, and share what you learn with others.



Ask questions

Contact officials, attend meetings, and ask how data is collected, used, shared, and protected.



Request transparency

Use public records laws to request policies, contracts, logs, audits, and other public information.



Get involved

Comment at meetings, join local groups, and encourage others to participate.



Speak up

Share your perspective respectfully and let leaders know what matters to you.



Support strong policies

Advocate for clear rules, limits on use, independent oversight, and strong privacy protections.

What to look for in local decisions



Clear purpose

The problem is defined, and the technology is necessary to address it.



Narrow use

Use is limited to specific purposes and not expanded without public approval.



Strong safeguards

Data is secure, access is limited, and retention is reasonable.



Independent oversight

Audits, reporting, and accountability are built in.



Public involvement

Communities are informed early and have real opportunities to be heard.



Regular review

Policies, outcomes, and impacts are reviewed and adjusted as needed.

Get connected with BPA



Visit our website

bendprivacy.org



Join our newsletter

<https://tinyurl.com/BPA-newsletter>



Attend events

Join community meetings and educational events in Bend.



Support the mission

Share, volunteer, and help us build a more private and transparent community.

◆ We are stronger together.
Thank you for being part of the change. ◆



BEND
PRIVACY ALLIANCE

*Watching the
watchers since 2026*



◆ Our privacy. Our rights. Our community.
Let's get it right—together. ◆



TAKE ACTION TODAY



Why this conversation matters

Technology will keep evolving. Our community values don't have to. By staying informed and involved, we can make sure innovation serves the public good—today and for generations to come.

THIS CONVERSATION CAN HELP:



Build understanding

Learn how local technology works and how data is used.



Identify concerns

Share what worries you and hear from others.



Explore solutions

Consider practical ideas for better policies and stronger safeguards.



Inform decisions

Community input can shape the choices our leaders make.



Strengthen our community

Privacy, transparency, and accountability benefit everyone.

KEY TAKEAWAYS



ALPR collects data about all of us.
It's designed to scan constantly—which means everyone is captured.



Without limits, risks grow.
Mass data collection can lead to abuse, misuse, and loss of civil liberties.



Oversight and policy protect us.
Clear rules, transparency, and accountability are essential.



Our voices make a difference.
Engaged communities build better policies and a stronger Bend.



Privacy is a community value.
Protecting privacy protects dignity, freedom, and the future we share.



An informed community is an empowered community.
THANK YOU FOR BEING PART OF THIS IMPORTANT CONVERSATION.

Questions

Event resources and follow-up information

? QUESTIONS & RESOURCES

Event resources



Slides and full citations



Bend surveillance source library



ALPR and retail-surveillance explainers



Protect Yourself guide



Proposed ordinance principles

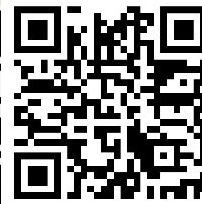


Public-comment and contact information



Corrections and updates

Scan for event resources



Bend Privacy Alliance

jonathanwestmoreland.com

bendprivacyalliance.org

coprivacy.org

*Slides, sources, updates,
and contact information in one place.*



If we cannot answer a question tonight, we will update the record.



BEND
PRIVACY ALLIANCE

◆ *Watching the watchers since 2026.*



PUBLIC NOTICE. PUBLIC RECORD. ACCOUNTABLE RULES.