Written Testimony — SB 1516

House Committee on Rules

Submitted by: Jonathan Westmoreland, Bend, Oregon
Position: Support only with amendments (guardrails package)

Chair Bowman and Members of the Committee:

My name is **Jonathan Westmoreland** and I live in **Bend, Oregon**. I've worked in technology since **before Google existed**, and I've had hands-on roles deploying and operating **AI-capable camera systems**—enough to understand both their value and how easily they can be expanded beyond their original purpose.

I have consistently watched technology outpace legislation. One of Flock's patents describes a broad object-tracking system that can index people by attributes. **Flock also has a technology partnership with Axon, a major law-enforcement technology vendor.** Verra Mobility is a channel provider for Flock Safety and is currently being deployed in Bend after the city canceled their contract with Flock. I am skeptical of feature creep in an AI, always-on tracking layer where one software update can turn these systems from a neutral crime-solving tool into mass surveillance infrastructure.

I support legitimate, targeted public-safety use of ALPR systems when they are narrowly tailored and accountable. However, **SB 1516 still risks enabling mass location surveillance** unless it includes a cohesive, enforceable set of guardrails.

Below is the **package of safeguards** I'm asking you to adopt. Each item matters on its own; together they prevent scope creep, reduce misuse risk, and preserve investigative utility.

1) Data minimization: define ALPR data narrowly

Request: Limit "captured license plate data" (or equivalent term) to only what is necessary:

- Plate characters (plate number)
- Timestamp (date/time captured)
- Location (camera location or GPS point)
- Camera/device identifier (for auditing)

Request: Prohibit vague catch-alls such as **"any other related data or information."**

Request: Prohibit collecting, deriving, or storing unrelated identifiers or personal attributes from images (including through future software/model updates).

2) Retention: automatic deletion on a short timeline unless case-linked

Request: Require **automatic deletion within a short window (e.g., 72 hours)** unless the record is affirmatively linked to:

- A specific criminal investigation and case number, or

- A documented investigative purpose meeting a clear statutory standard

Request: Any retention extension must be **documented and auditable** (no informal or indefinite "just in case" stockpiling).

3) Access controls and audit logs: make misuse detectable and enforceable

Request: Require, at minimum:

- **Role-based access controls** (least privilege)
- **Strong authentication (MFA)** for all access
- **Search logging** capturing: user identity, time, search terms, purpose, and case number or documented reason
- **Regular audits** with clear consequences for improper access and misuse

4) Sharing limits: restrict cross-jurisdiction and downstream use

Even responsible local programs can become a distributed surveillance network if sharing is broad or informal. Request:

- Prohibit **bulk sharing** and broad third-party access
- Limit disclosure outside the collecting agency to narrow, documented circumstances
- Require disclosure to be **logged, auditable, and tied to a specific statutory purpose**
- Prohibit vendor or third-party repurposing of ALPR data beyond authorized use

5) Security requirements: protect the data end-to-end in practice

ALPR data is sensitive because it can reveal patterns of life—where people live, work, worship, seek medical care, or spend time. **If ALPR systems or vendor platforms are breached, this data can be exploited for stalking, harassment, intimidation, doxxing, or targeting vulnerable communities.** A breach can also undermine investigations by exposing law-enforcement activity and search patterns.

Request: Require enforceable security controls, including:

- Encryption **in transit and at rest**
- **End-to-end encryption (E2EE), clearly defined in statute, with keys controlled by the Oregon customer (or another clearly defined endpoint)**, so "encryption" can't be satisfied by minimal or ambiguous implementations
- Secure key management appropriate to sensitive data
- Vendor accountability for security practices and incident response
- Requirements that are **verifiable and enforceable** (not aspirational "best practices")

6) Transparency: public accountability without exposing sensitive details

Request: Require regular public reporting (annual or comparable) of aggregate metrics such as:

- Total scans and general retention practices
- Number of searches and categories of purpose
- Number and categories of disclosures/sharing
- Audit/compliance outcomes (in aggregate)

Closing

SB 1516 can be a meaningful step **only if it prevents routine, warrantless location tracking at scale** and includes enforceable technical and policy guardrails. I respectfully ask you to adopt this safeguard package so ALPR use in Oregon remains narrow, accountable, and consistent with democratic oversight.

The laws written today should prioritize the digital safety and freedom of the law-abiding public over the business models of surveillance companies and the convenience of unchecked data access.

If the committee is not able to amend SB 1516 to address these concerns, I urge you to vote no and revisit this issue in the next legislative session with a stronger, enforceable framework.

Respectfully submitted,
Jonathan Westmoreland
Bend, Oregon