To: Chair Bowman and Members of the Committee

Re: SB 1516 - Follow-up Written Testimony (ties together my prior written testimony, my emails to the committee, and my virtual testimony)

Chair Bowman and Members of the Committee,

My name is Jonathan Westmoreland and I live in Bend. Thank you for the opportunity to submit this follow-up written testimony. This document is intended to tie together ([1]) my earlier written testimony, ([2]) the individual emails I sent to committee members asking you to champion specific guardrails, and ([3]) my one-minute virtual testimony.

My core point is simple:

SB 1516 should be evaluated not only as a snapshot of today's ALPR systems, but as governance for what these systems can become tomorrow. Vendors routinely add or change capabilities through remote software updates, and "ALPR" vendors increasingly integrate additional surveillance modalities beyond license plates.

This is not an argument against targeted, accountable ALPR use for legitimate public safety. It is an argument for ensuring SB 1516 has durable guardrails that remain enforceable as technology evolves and as vendor incentives push toward expansion.

[1]) The question the bill must answer: Will it still protect Oregonians after a remote software update?

Software-defined systems change after purchase. That is the nature of modern technology. A clear example is Tesla's October 2015 software update (Version 7.0) that activated Autopilot features through an over-the-air rollout.

`Source: https://www.motorauthority.com/news/1100476_tesla-version-7-0-software-update-activates-first-autopilot-features`

The relevance to SB 1516 is not Tesla itself; it is the governance lesson:

- Capabilities can be added or expanded later.
- Rollouts can happen at scale.
- The public may not know what changed until after impacts occur.

ALPR deployments are also software-defined. In procurement materials for LPR systems used by Bend, the platform explicitly includes ongoing "software updates" and even "automated ... software update management."

That means the bill cannot rely on assumptions about what a system does today. The bill must ensure that if an ALPR system later expands what it collects, infers, retains, or shares, those expansions remain constrained by enforceable law.

[2]) "ALPR" no longer always means "just license plates": electronic signature / device-identifier tracking (SignalTrace)

In my virtual testimony I referenced "device signatures." This is not hypothetical.

Leonardo/ELSAG markets "SignalTrace" as an electronic signal intelligence capability that can help identify suspect people or vehicles even when a license plate number is not known.

`Source: https://www.leonardocompany-us.com/lpr/elsag-signaltrace`

Leonardo also describes SignalTrace as enabling identification of electronic devices (such as smartphones and RFID tags) that may be linked to suspects, using sensor technology.

`Source: https://www.leonardocompany-us.com/lpr/eoc-plus-product-sheet`

In plain terms, the privacy risk is straightforward:

- If a system can detect device-emitted identifiers and correlate them over time,
- and those identifiers can be linked to a vehicle, route, or person,
- then the system can enable long-term location tracking even when the plate is missing, changed, obscured, or never captured.

That creates a parallel surveillance dataset about movements and associations that is qualitatively different from a photo of a plate. It can also create "association" intelligence (who travels with whom), because multiple devices traveling together can form a persistent traveling cluster that is more identifying than a single plate read.

This is exactly why my central question matters: if SB 1516 is written to regulate "captured license plate data," but systems evolve to capture and correlate additional identifiers, then the law may fail to protect Oregonians from mass location surveillance conducted through adjacent data streams.

[3]) Vendor incentives: commercial datasets and downstream sharing pressures

My spoken testimony used the shorthand that vendors "monetize data." I want to keep this written record precise and rooted in documentary facts.

A key factual point: some LPR platforms explicitly include access to "commercially acquired national vehicle location data" as a subscription feature. In Bend-related LPR procurement documentation, an "Investigative Data Platform" subscription includes "Commercial LPR Data access" and "access to all Vigilant commercially acquired national vehicle location data." [1]

Whether one calls that "data brokering" or "commercial LPR data services," the incentive structure is the same: the business model supports collecting, aggregating, and monetizing vehicle location detections and access to them. That creates predictable pressures toward:

- longer retention,
- broader sharing,
- more integrations, and
- expanded analytics and correlation.

Those pressures do not mean ALPR cannot be used responsibly. They do mean SB 1516 needs bright-line guardrails that do not depend on vendor goodwill, marketing terms, or fluctuating contract language.

[4]) I support the -15 / A15 amendment’s end-to-end encryption definition, and why it matters

I want to clearly restate what I said in my testimony: I support the -15 amendment (A15) adding a definition of "end-to-end encryption."

According to the published staff measure summary, A15 adds a definition of end-to-end encryption "to mean a method of data encryption that ensures only the owner of the captured license plate data possesses the capability to decrypt, access or grant access to the data."

```
Source: https://olis.oregonlegislature.gov/liz/2026R1/Downloads/CommitteeMeetingDocument/315765
```

Why that definition matters:

- If "end-to-end encryption" is not defined, it can become a marketing label rather than an enforceable security requirement.
- If it is defined, auditors, agencies, courts, and the public have a common standard to evaluate compliance.
- The definition directly addresses the risk that a vendor could retain decryption capability (or later add it via update) in a way that defeats the public’s understanding of end-to-end encryption.

More broadly, the staff summary indicates A15 also addresses vendor contract requirements, limits vendor use/licensing of captured data, and requires certain audits to be made public quickly.

```
Source: https://olis.oregonlegislature.gov/liz/2026R1/Downloads/CommitteeMeetingDocument/315765
```

Those are directionally aligned with the guardrails I have advocated in my prior written testimony and emails: enforceable technical protections, enforceable limits on secondary use, and accountability through auditability.

[5]) The cohesive guardrails SB 1516 should guarantee (and why each is necessary)

The bill should function as a durable safety envelope that remains enforceable as systems evolve. The guardrails I urged in my written testimony and follow-up emails can be summarized as:

A) Data minimization (collection limitation) Require ALPR collection be limited to narrowly necessary fields (for example: plate, timestamp, location), and prevent expansion into vague categories like "any other related data" or derived inferences unless explicitly authorized, narrowly defined, and justified.

This aligns with established privacy principles: collect only what is directly relevant and necessary, and limit data fields to what is relevant. [[2]]

B) Short retention with deletion by default Require automatic purging on a short schedule unless a record is affirmatively linked to a case-specific investigative purpose. Deletion by default is the key, because retention creep is one of the most common ways surveillance becomes mass surveillance.

The same policy template emphasizes designing systems for automatic purging after a specified retention period. [[3]]

C) Strong access controls, reason-for-access, and real auditing To prevent misuse and enable accountability, every search should be tied to:

with regular review and meaningful consequences for misuse.

- an identified user,
- a documented reason/purpose, and
- where applicable, a case number,

This is consistent with best-practice guidance that asks whether access identifies the user and whether the identity is retained in audit logs, and whether an audit trail is maintained. [[4]]

D) Hard limits on sharing and downstream use Sharing is where targeted use can become broad surveillance, especially when data flows across jurisdictions or to federal agencies. The bill should set strict legal thresholds, transparency requirements, and enforceable constraints so sharing cannot expand quietly through policy changes, MOUs, or software integrations.

E) A defined, enforceable encryption standard (including support for A15's E2EE definition) Encryption is not a box-check. A definition like A15's makes it possible to verify whether only the owner can decrypt and grant access.

`Source: https://olis.oregonlegislature.gov/liz/2026R1/Downloads/CommitteeMeetingDocument/315765`

[6]) Why remote updates plus device-signature tracking makes guardrails urgent

If lawmakers take away only one point from my testimony, I hope it is this:

ALPR governance must be designed to hold even when:

- the vendor changes software,
- the system gains new capabilities,
- the system integrates additional sensors/data streams, and
- the system's data becomes more linkable and more revealing over time.

Leonardo's SignalTrace marketing makes plain that systems are evolving to identify people/vehicles through electronic devices even without plate reads.

`Source: https://www.leonardocompany-us.com/lpr/elsag-signaltrace`

And Bend-related procurement documentation shows ongoing software update pathways and access to commercial vehicle location datasets. [5] [6]

This combination (remote updates plus multi-modal correlation plus commercial location datasets) is exactly the recipe for feature creep that turns a narrow investigative tool into mass location surveillance infrastructure.

7) Request to the Committee

I respectfully ask you to ensure SB 1516 includes a cohesive, enforceable bundle of guardrails that remain durable after remote updates and technology expansion:

[1]) Codify strict data minimization (and narrow any "other data" language). [2]) Require short retention with deletion by default and limited, logged exceptions. [3]) Mandate strong access controls, reason-for-access logging, and meaningful audits. [4]) Impose strict limits on sharing and downstream use, with clear thresholds and accountability. [5]) Adopt and keep enforceable the -15 / A15 definition of end-to-end encryption.

`Source: https://olis.oregonlegislature.gov/liz/2026R1/Downloads/CommitteeMeetingDocument/315765`

If the bill cannot be amended to accomplish these protections, then I urge you to vote no on SB 1516 as written and revisit the bill in the next session with stronger, technology-realistic guardrails.

Thank you for your time and for your public service.

Respectfully submitted,

Jonathan Westmoreland Bend, Oregon

References (documentary citations used in my prior testimony/emails)

[1] Bend-related procurement documentation: "Investigative Data Platform" includes commercial LPR data access and access to Vigilant commercially acquired national vehicle location data.

[2] LPR policy development template: data minimization principle (collect only directly relevant/necessary fields).

[3] LPR policy development template: retention and automatic purging guidance.

[4] CJIS Security Policy: auditing guidance (identify user access; retain in audit logs; maintain audit trail).

[5] Bend-related procurement documentation: software updates and automated software update management.

[6] Bend-related procurement documentation: commercial vehicle location datasets access.