1. “The system is limited, short-term, and privacy-protective.”

OPD claim (slides 5-6, 14):

- Flock is *not* tied to PII, not facial recognition, not immigration or traffic enforcement, and not shared with federal or out-of-state agencies.
- Data is retained only 30 days then deleted; cameras capture “only plates” and “vehicle data, not people.”
- Flock records are public but supposedly low-risk because they aren’t “personally identifiable.”

Facts:

- **ALPR data *is* personally identifying when combined with other common data.** The Brennan Center and ACLU both treat ALPR data (plate + time + GPS location) as *personal information* because it creates a detailed history of where specific people travel. Courts and attorneys general have explicitly said ALPR travel histories can count as “personal information” about individuals. Brennan Center for Justice+1
- **Washington now has a binding trial-court ruling that Flock data is a public record.**
  A Skagit County judge ruled that ALPR images and associated data are subject to Washington’s Public Records Act. In response, cities like Redmond and Lynnwood paused their Flock programs, explicitly citing the risk that *anyone* can request the plate-level data and that agencies “have no ability to control who is getting access…and how they’re using it.” Washington State Standard
- **Washington has zero statewide ALPR regulations right now.**
  At least 16 states regulate ALPRs; Washington does not. Lawmakers are only just starting to draft basic guardrails, including retention limits and use restrictions, after revelations about Flock data reaching federal immigration authorities. Washington State Standard
- **Flock’s own systems now capture far more than “just plates.”**
  Investigative reporting shows Flock cameras and AI are trained to detect license plates, vehicles *and people*, including clothing, and Flock material references detecting “race,” as well as audio events like gunshots or “screaming.” WIRED

Why it matters for council:

Even if Olympia configures Flock to the "least invasive" settings today, the *technical reality* is:

- The underlying system is already capable of much broader surveillance of people and behavior, not just plates.
- The data is legally a public record in Washington and may have to be turned over to *any* requester – stalkers, abusers, bounty hunters, data brokers – not just journalists and advocates.
- "No PII" and "30-day retention" are *policy choices* and *vendor settings,* not hard statutory protections. They can change with a contract amendment, a future council, a future chief, or a quiet vendor feature change.

This is functionally a city-operated location-tracking system on every resident with a car, and Washington currently has almost no legal guardrails for how that data can be used or misused.

---

2. "We don't share with federal / immigration agencies."

OPD claim (slides 5 & 7):

- Flock is "not used for immigration enforcement" and "not shared with federal or out-of-state law enforcement."

Facts:

- **A University of Washington report found at least eight Washington agencies directly shared Flock networks with U.S. Border Patrol** in 2025 (Arlington, Auburn, Yakima, Lakewood, Richland, Sunnyside, Wenatchee, and Benton County Sheriff). KUOW+1
- The same report found evidence of **"back door" access**, where Border Patrol accessed data from agencies that had *not* intentionally granted access, and **"side door" searches,** where local police ran queries on behalf of immigration authorities. Dailyfly News
- Washington's Keep Washington Working Act restricts local police cooperation with civil immigration enforcement. The UW researchers explicitly warn that this pattern of Flock sharing may be inconsistent with state law. Dailyfly News+1

- **Flock's "National Lookup" feature is the mechanism that allows this.** KUOW and UW describe "National Lookup" as the tool that lets any Flock-enabled agency search plate data from other agencies around the country. Local departments admitted they didn't fully understand that their sharing settings opened the door to federal access. KUOW

Why it matters for council:

- OPD may sincerely believe they are not sharing with federal immigration agencies. But the *Washington-specific* evidence shows that agencies using Flock have already, in practice, shared data with U.S. Border Patrol through misconfigured settings, "back door" access, or officers running queries for federal partners.
- That means **"we don't share with immigration" is not a technical guarantee.** It is a check box in a vendor UI that other Washington agencies have already gotten wrong – with potential conflicts with state law.

If other Washington departments misunderstood the system's sharing controls, we should assume Olympia is vulnerable to the same misconfigurations, especially over years of staff turnover. That is not an acceptable risk for a city that has adopted sanctuary-style policies.

---

3. "It's just 30 days – and mostly worthless data – unless it hits on a crime."

OPD claim (slide 6):

- 30-day retention protects privacy.
- Anything "not associated with a crime" is automatically deleted and "unrecoverable."
- Volume: ~4 million images every 30 days in Olympia.

Facts:

- From OPD's own slide: **~4,000,000 images every 30 days** in Olympia. That's ~48 million plate reads per year for a city of ~58,000 people – *hundreds* of scans per resident per year, even if you only count residents.
- **Their arrest numbers are tiny compared with the volume of surveillance.** OPD's slide shows **110 "Flock-assisted arrests" and 29 stolen vehicles recovered**

since August 2024. Over roughly a year of data at 4M reads per month, that's on the order of **2 arrests per 1,000,000 plate scans** even under generous assumptions.

We're scanning tens of millions of license plates each year to generate a few dozen cases. That is a massive surveillance footprint for a very small marginal benefit.

- The RAND report on ALPRs notes that **passive, bulk collection of plate data has "wholly speculative" future value** for most of those records – they are retained "just in case," not for a specific, pre-established investigative need. Office of Justice Programs
- The ACLU's "You Are Being Tracked" report warns that increasing camera coverage, longer retention, and broad sharing create "enormous databases" of location data that allow police to reconstruct a detailed picture of people's lives and chill free speech and association. ACLU Assets

Why it matters for council:

For tens of millions of scans of innocent people, we are getting a trickle of hits. Even if a handful of those are serious crimes, you have to decide whether mass location tracking of the entire driving population is a proportionate and acceptable way to get that marginal benefit – especially when the same data is legally a public record and can end up in anyone's hands.

---

4. "There's no AI or predictive policing here."

OPD claim (slide 5-6):

- Flock is "NOT predictive policing."
- They emphasize objective plate reads, not AI or biometrics.

Facts:

- **Flock as a company is openly rolling out AI products on top of the same underlying data.**
    - "Enhanced LPR" uses AI to link suspect vehicles to multiple crime scenes and highlight crime "hotspots." Flock Safety
    - **Flock Nova** is an AI analytics platform that unifies RMS, CAD, LPR and other datasets, surfaces patterns, and generates "intelligence" from plate data. Flock Safety+1

    - Flock blogs describe “AI that works in the background, doing pattern recognition, prioritization, and insight delivery,” including plain-language searching (“blue SUV with racing stripe”) and automatic pattern detection across huge datasets. Flock Safety+1

- **The ACLU reports that Flock is now using AI to scan nationwide vehicle movement patterns and proactively flag “suspicious” behavior.**
  Flock funnels plate reads from customers across the nation into a central database and runs analytics to identify vehicles whose movement patterns an algorithm deems “suspect,” then alerts police – shifting from investigating specific leads to *generating* suspicion. American Civil Liberties Union+1
- A Wired/404 Media investigation shows Flock uses overseas gig workers and AI systems not just to read plates but to classify vehicles, people, clothing, and audio events (“gunshot,” “screaming”) for training its models. WIRED

Why it matters for council:

Even if OPD has *not yet purchased* Nova or Enhanced LPR, the architecture is already in place:

- Olympia’s Flock data is going into an ecosystem that is actively being upgraded with AI capabilities aimed at pattern analysis and movement-based suspicion.
- Once the infrastructure and contract are in place, **it is very easy for a future chief or council to “flip on” these AI features with a software add-on, especially under political pressure after a high-profile crime.**

OPD can truthfully say they are not *currently* using predictive AI. But the vendor is already marketing AI tools that turn this into a suspicion-generation engine. By keeping this contract, you are entrenching an infrastructure that is designed to evolve toward predictive policing, whether we like it or not.

---

5. “Flock isn’t linked to other surveillance – it’s just our cameras.”

OPD claim (slide 5 & 10):

- Flock is not shared with federal or out-of-state law enforcement; it’s presented as a local, bounded system.

Facts:

- **There is now a direct integration between Flock and Amazon's Ring.**
  In October 2025, Ring announced a partnership with Flock where police agencies using Flock's Nova or FlockOS platforms can request video from Ring users through the Neighbors app. Ring users in a geographic area see requests and can share footage, and Flock's system has already been used by federal agencies like the Secret Service, Navy, and ICE according to a letter from Sen. Ron Wyden summarized by The Verge. The Verge
- For years, Ring has been criticized for providing video to police without a warrant in some circumstances, and even after it shut down one police-request feature, it kept an "emergency" carve-out for warrantless data sharing. The Verge

Why it matters for council:

Olympia's Flock network is **not an island**:

- It sits in the middle of a growing web that now includes privately owned doorbells and cameras on people's front doors and porches.
- The line between "public right-of-way cameras" and "private home surveillance feeding the same investigative platform" is already blurring.

Do you want Olympia Police to be plugged into a national system that can reach into people's private doorbell cameras and centralize that footage alongside our mass vehicle tracking, especially as AI analytics get layered on top?

---

6. "Abuse is not a real concern – we have policies and audits."

OPD claim (slides 9–10):

- There is a public search audit, a transparency portal, and a policy limiting use to legitimate investigations.
- A search reason is required, which they imply prevents improper access or misuse.

Administrative controls such as audit logs, policies, and search-reason fields are not technical safeguards. They do not prevent unauthorized or inappropriate queries; they only record them after the fact. From an information-security standpoint, these controls cannot meaningfully mitigate risks inherent to mass collection of sensitive location data.

a. Audit logs provide retrospective visibility, not prevention.

Audit logs are a **forensic control**, not a **preventative security control**. They:

- record actions *after* they occur,
- require manual review to detect issues, and
- cannot stop an authorized user from running an unauthorized or inappropriate query.

This is a well-established principle in professional security standards, including NIST SP 800-53, which classifies logging under **"detection"**, not **"protection."**

b. A required "search reason" is an integrity requirement, not a security safeguard.

A search-reason field:

- does *not* restrict what can be queried,
- does *not* validate the legitimacy of the reason,
- and can be satisfied with any entry.

From a data-security perspective, this is comparable to entering a comment before performing an administrative action. It does not constitute true access control.

c. Transparency portals do not mitigate the underlying risks of scale and sensitivity.

Security risk increases with:

- the **volume** of data,
- the **sensitivity** of the data, and
- the **number of people with access**.

Flock captures **continuous, non-incident-based sensitive location data** for the entire population of Olympia. This creates high-value data regardless of whether a transparency portal exists.

d. Policies cannot substitute for technical enforcement mechanisms.

Policies rely on **human compliance**, not technical restrictions.

Effective prevention requires:

- purpose-based access controls enforced by software,
- query restrictions that cannot be bypassed,
- real-time anomaly detection, and
- enforced data-minimization rules.

Flock does **not** provide granular, purpose-restricted access controls. If a user has access to the system, they can query **any plate**, at **any time**, and results will be returned.

e. Audit and policy controls do not mitigate Washington PRA exposure.

Under Washington's Public Records Act (RCW 42.56):

- ALPR data is a **public record**,
- and must be disclosed unless tied to an active investigation.

A 2024 **Skagit County Superior Court ruling** confirmed that **Flock ALPR data is disclosable**, resulting in:

- **Redmond pausing its Flock program**,
- **Lynnwood pausing its Flock program**, and
- emergency reviews in other cities.

Audit controls cannot prevent legally mandated release of sensitive location data.

f. Data-security best practice centers on data minimization — which ALPR systems contradict.

Under NIST, ISO 27001, and modern data-protection frameworks, one of the highest-value protective principles is **collect only what is necessary**.

ALPR systems:

- collect data on **all vehicles**, not suspects,
- store information regardless of investigative need,
- retain sensitive location data for a fixed period (30 days), and
- generate a large, high-risk dataset by design.

No audit mechanism can compensate for excessive data collection at this scale.

Why this matters for Council:

- Audit logs **detect**, not prevent.
- Policy-based controls rely on human behavior, not security engineering.
- Search-reason fields do not restrict access.
- Large, sensitive datasets dramatically increase inherent risk.
- Washington's PRA requires disclosure of ALPR data, regardless of audit controls.
- From a data-security perspective, the only effective mitigation for unwanted access or disclosure is **not to collect the data at all**.

---

7. "The tech is clearly legal and settled."

OPD claim (slide 55):
By presenting Flock as compliant with all laws and mentioning "adheres to all state laws," the deck suggests the legal questions are resolved.

Facts:

- In **Norfolk, Virginia**, a judge ruled that collecting and using data from 172 Flock cameras to track vehicles constituted a **Fourth Amendment search**, and suppressed that evidence when it was collected without a warrant. Wikipedia
- Washington's **Skagit County ruling** held that ALPR/Flock data is a public record that must be disclosed under the Public Records Act, prompting some cities to suspend programs and others to lobby for *less* transparency. Washington State Standard
- Washington legislators are now actively drafting ALPR legislation precisely because the current legal landscape is unsettled and troubling, particularly around immigration, data sharing, and public disclosure. Washington State Standard+1

Why it matters for council:

- You are being asked to **double down** on a technology whose constitutional status, public-records status, and state-law compliance are *actively being litigated and rewritten right now*.
- If the Legislature tightens rules (for example, requiring warrants for certain queries or limiting sharing), Olympia could end up paying to deploy infrastructure that later must be drastically curtailed or ripped out.

It is fiscally and legally reckless to expand a system that is under current legal challenge and likely to be heavily regulated in the next session. The safest course is to step back, not double down.

---

8. "But don't the benefits outweigh the risks?"

You can pre-empt OPD's "110 arrests" and "success story" slides (slides 18-22).

Key points:

1. **Tiny yield vs. massive dragnet.**
    - ~4M scans per month, ~48M per year, to produce 110 arrests and 29 recovered cars.
    - That is a dragnet on essentially every driver in the city to get a small number of additional cases. The question is not "are there *any* success stories?" but "is this proportional and necessary compared to less intrusive options?"
2. **Benefits are real but not unique to Flock.**
    - ALPR can help recover stolen cars or locate specific suspect vehicles. But those benefits can often be achieved with **more targeted, less centralized tools** – for example, limited ALPR on patrol cars or at specific known hot spots, with much stricter policies, shorter retention, and no integration into a nationwide analytics platform.
3. **Risks are structural and hard to undo.**
    - Once you have dozens of fixed, networked cameras feeding a centralized vendor database, a future council or chief can easily expand retention, sharing, and AI features with a click. Rolling this back later is politically and contractually harder than simply not expanding it now.
4. **Alternative investments.**

- Every dollar we spend on embedding Olympia into a national surveillance infrastructure is a dollar not spent on things we know reduce harm – like mental health response, traffic calming, lighting, youth programs, or investigators dedicated to specific crime types.

---

9. "Public disclosure of Flock data is just like any other police record."

OPD claim (slides 13–15):

- Flock data "falls under the same disclosure requirements as many other police records."
- PRA access is "not unique."
- Active investigations are exempt.
- OPD will "safety-plan" with DV survivors and "follow up" if stalking is suspected.

This claim is technically accurate but functionally misleading.

ALPR data is *fundamentally different* from other police records – and Washington's Public Records Act makes it extraordinarily dangerous.**

a. **ALPR data is categorically different from standard police records.**

   OPD compares Flock data to body cam video, digital evidence, and police reports.

   This is false equivalence.

   - **Police reports** are event-based and investigator-generated.
   - **Body cam video** documents specific encounters.
   - **Digital evidence** exists only in relation to an identified incident.

   Flock is completely different:

   - It creates **continuous, indiscriminate, citywide surveillance**.
   - It captures **location and movement patterns of thousands of people who are not suspected of anything**.
   - It allows reconstruction of a resident's **daily routines, home address, workplace, healthcare visits, religious attendance, and relationships**.

   No other routine police record has this sensitive "pattern of life" quality.

This is why national privacy groups classify ALPR data as **high-risk location intelligence**, not ordinary evidence.

b. Washington's Public Records Act has no privacy exemption that protects ALPR data.

This is the most important point.

Washington's PRA is one of the strictest disclosure laws in the country, and **there is no statutory exemption broad enough to protect bulk location data**.

This is why:

A Skagit County judge ruled in 2024 that Flock and ALPR data *must* be disclosed under the PRA.

As a result:

- **Redmond paused their Flock program**
- **Lynnwood paused their Flock program**
- Other WA cities launched emergency reviews

Those cities cited the same issue:

"We have no ability to control who requests this data or how they use it." – Redmond PD (WA State Standard reporting)

This is **not** true of body cam footage or police reports, which typically relate to specific, documented incidents.

This is **uniquely** dangerous for ALPR.

c. ALPR data creates a practical roadmap for stalkers, abusers, and harassers.

OPD says they will "check plates against survivor records" and "investigate suspected stalking."

This is reactive, not protective.

A stalker or abuser only needs:

- a license plate
- to know the PRA exists

Under current Washington law, they can request:

"All hits on plate ABC123 for the last 30 days."

They will legally receive:

- timestamps

- GPS location
- multiple angles
- patterns of presence
- nightly parking locations
- visits to clinics, shelters, workplaces, or partners' homes

OPD's "follow up" happens **after** the data is already released.

You cannot "un-release" location data.

This is why DV advocates consider ALPR data among the **highest-risk categories** of information.

d. Exempting active investigations protects the City—not the public.

OPD says plates tied to an active investigation are exempt.

But most people at highest risk of harm:

- DV survivors
- trans or queer residents fleeing unsafe homes
- people seeking reproductive or gender-affirming care
- immigrants avoiding surveillance
- activists and journalists
- people with stalkers

do not have active cases open.

Their safety is not meaningfully protected by an "active investigation" exemption.

e. OPD's own slides reveal how massive and risky this dataset is.

Slide 14 admits:

- **~4 million images every 30 days**
- Residents may view images "at no cost"

This means:

- ~48 million images per year
- In a city of ~58,000
- All legally disclosable
- All containing sensitive travel data

- None protected by a general privacy exemption

No other Olympia police system exposes the public to this level of potential harm.

f. Washington has already seen ALPR misuse, sharing failures, and "back-door access."

The University of Washington's 2025 report documented:

- **8 Washington agencies gave U.S. Border Patrol access to their Flock data**
- Several agencies *believed* they weren't sharing when they actually were
- "Back door" access occurred when federal agencies used other departments to query local data
- "Side door" access occurred when local officers ran plate searches for federal agencies
- These patterns may conflict with WA's Keep Washington Working Act

This is not theoretical.
It has already happened here.

The risk is not OPD's staff – the risk is the entire **data-sharing ecosystem** and Washington's weak statutory privacy protections.

g. No combination of policies, audits, or internal procedures can mitigate PRA disclosure risk.

OPD's measures – checking plates, conducting DV follow-up, and investigating suspicious requests – all occur **after** the data is out the door.

Once released, the harm is permanent.

That means the only real safeguard against PRA-mandated disclosure is:
Do not create the data in the first place.

Why this matters for Council:

ALPR data is unlike any other police record because:

- It is **indiscriminate**, not incident-based.
- It captures **highly sensitive location data**.
- It is **legally public** under WA law.
- It has **already been misused statewide**.
- It creates **unique, irreversible harms** for DV survivors, immigrants, vulnerable residents, and anyone who drives a car.

- OPD cannot stop disclosure once the request is valid.
- No internal policy can override state law or prevent misuse of released data.

OPD's statement that "public disclosure is standard" is technically true but substantively false.
ALPR data is uniquely dangerous under Washington's PRA, and Olympia cannot safely operate a citywide mass-surveillance system that the law requires to be released to anyone who asks.

---

10. "Flock is secure – encryption, 2FA, ISO 27001, and CISA commitments protect the data."

OPD claim (slide 16 on cybersecurity):

- The City of Olympia utilizes two-factor authentication on all City computers.
- OPD uses two-factor authentication on all Department Mobile Computer Terminals.
- Flock is aligned with CISA's "Secure By Design" principles.
- Flock submits vulnerability reports to MITRE and the National Vulnerability Database (NVD).
- Flock uses AES-256 encryption and maintains ISO 27001 compliance.

These points describe standard IT hygiene – not meaningful protections against the real risks of mass location surveillance. The primary danger is not hacking; it is the existence, scope, and mandatory disclosability of the data itself.

a. **Two-factor authentication does not mitigate systemic surveillance risk.**
   2FA protects employee logins – not residents.
   It prevents unauthorized staff access, but it does **nothing** to address:
   - the **volume** of data collected,
   - the **sensitivity** of location patterns,
   - the **legal requirement to disclose data under the PRA**,
   - the **risk of misuse by authorized users**,
   - or the **structural risks of mass surveillance infrastructure**.

   Every major data breach of the last decade – Equifax, OPM, T-Mobile, AT&T, Marriott – occurred at organizations *also using 2FA*.
   2FA is basic, not a safeguard.

b. **CISA "Secure By Design" is a voluntary pledge, not an enforceable obligation.**
   CISA's initiative is a **public commitment**, not a regulatory standard.
   It does **not**:
   - restrict what data Flock can collect,

- prevent the expansion of AI analytics,
- limit data sharing across jurisdictions,
- override Washington's PRA disclosure mandates,
- or constrain vendor-driven feature expansion.

This pledge in no way addresses the **core civil liberties threat** posed by ALPR systems.

c. Submitting vulnerabilities to MITRE's National Vulnerability Database is standard industry procedure, not evidence of exceptional security.

Any company producing software is expected to disclose vulnerabilities to NVD. This is not a special protection – it is the **bare minimum** of responsible security practice.

It also does not prevent:

- configuration errors,
- policy failures,
- misuse by authorized personnel,
- data-sharing mistakes (which have already occurred in WA),
- "back door" or "side door" access by other agencies.
  Past misuse of ALPR in Washington demonstrates the risk is **governance**, not software patching.

d. AES-256 encryption and ISO 27001 compliance secure data at rest – but do not reduce the danger of the data being created in the first place.

Encryption protects data from external attackers – not from:

- lawful public disclosure (PRA),
- authorized misuse,
- political shifts in data-sharing policy,
- federal subpoenas or warrants,
- Flock's own integrations with other private surveillance networks,
- future analytic upgrades using AI-enhanced vehicle fingerprinting.

An encrypted mass-surveillance database is still a mass-surveillance database. ISO 27001 simply certifies that Flock has **repeatable security processes** – not that its operations are safe, ethical, or compatible with Washington's transparency laws.

e. The primary cybersecurity threat with ALPR is not external hackers – it is the mandated release and internal use of sensitive location data.

OPD's cybersecurity framing treats Flock as if the danger were someone "breaking in."

But the real threat is:

- **the scale of collection** (~4 million images every 30 days),
- **the legal obligation to disclose** if requested,
- **the sensitivity of the insights** (home, work, clinics, shelters, visitation patterns),
- **authorized misuse** – which is historically the most common misuse of police databases,
- **data-sharing across agencies**, which in Washington has already exposed ALPR data to **U.S. Border Patrol**,
- **feature creep** as Flock expands AI tools and public–private integrations.
  No amount of encryption prevents these harms.

f. Real cybersecurity risk increases with scale – and Flock multiplies the City's attack surface dramatically.

The more data a system stores, the more valuable it becomes to:

- domestic abusers,
- stalkers,
- extremist groups,
- private investigators,
- bounty hunters,
- data brokers,
- malicious insiders,
- and sophisticated attackers.

Even if Flock's servers are secure, Washington's **Public Records Act** forces disclosure of this extremely sensitive dataset.
Encryption does not protect data from lawful release.

g. No cybersecurity certification or vendor pledge can fix the structural problem: ALPR generates highly sensitive, legally disclosable surveillance data about everyone.

This includes:

- innocent residents,
- city workers,
- activists,
- journalists,

- DV survivors,
- immigration-vulnerable communities,
- people accessing reproductive healthcare,
- youth and seniors,
- visitors,
- and anyone driving through Olympia.

Cybersecurity standards do not address the **far greater** risks created by mass location tracking combined with Washington's strict transparency laws.

Why this matters for Council:
The cybersecurity assurances OPD cites are **industry-baseline IT practices**, not meaningful safeguards. They do not:

- prevent PRA disclosure,
- prevent authorized misuse,
- limit surveillance scope,
- reduce the sensitivity of location intel,
- stop data-sharing errors (which have already occurred in WA),
- constrain future AI expansion,
- reduce civil liberties impacts,
- or meaningfully protect the public from harm.

OPD's cybersecurity points create the illusion of safety while ignoring the fundamental issue: the data Flock collects is too sensitive, too expansive, and too legally exposed to ever be made safe. The only real protection is not creating the dataset at all.

TLDR / Final Summary

OPD's own presentation shows that Flock captures **tens of millions of plate scans a year** in Olympia to produce a **very small number of investigative hits**, while creating an enormous, highly sensitive location database. Independent, Washington-specific findings now confirm that:

- **Flock data has already been accessed by U.S. Border Patrol in this state**,
- A **Skagit County judge ruled ALPR data is a public record** that *anyone* can request, and

- Flock is actively deploying **AI-driven analytic tools** that transform these systems from passive cameras into **behavior-profiling and suspicion-generating platforms**.

This is not a neutral public-safety upgrade. It is an expansion of Olympia's exposure to a **rapidly growing national surveillance infrastructure** in a state with **almost no guardrails**, **no statutory privacy protections**, and **mandatory public-disclosure obligations** that no policy or audit can override.

The risks here are **structural, irreversible, and substantially greater than the limited investigative benefits OPD has presented**. Once this infrastructure is entrenched, it is extremely difficult to scale back or dismantle.

Given the legal, technical, and civil-liberties risks now documented in Washington, the only responsible course of action is to step back from this contract – not expand or renew it.