

Why “Responsible Technologies” Is Not a Safeguard

Evidence Supporting Bend Privacy Alliance’s Position on Bend’s Draft 2027 Legislative Priorities

“Support expanding allowed uses of responsible technologies that strengthen public safety and service delivery.”

Bend Privacy Alliance believes this language creates a significant oversight problem.

The concern is not that every technology used by Bend Police is inherently the same, nor that Bend currently uses every capability available from its vendors. The concern is structural:

Bend has already built an interconnected public-safety technology platform whose capabilities can expand through software, licensing, configuration, integration and changes in law.

A legislative principle directing the City to support “expanding allowed uses” could make those expansions easier before the Council or public knows which specific authority is being expanded.

1. Bend already has a technology ecosystem, not a collection of isolated devices

Bend Police Department’s relationship with Axon extends well beyond body-worn cameras.

City purchasing records document a progression that includes:

- Axon body-worn cameras and Evidence;
- Axon Fleet 3 in-car cameras and mobile automated license plate recognition;
- Fusus camera and data integration;
- Axon Air drone software;
- Axon Records;
- Respond Plus;
- Auto-Transcribe;
- Auto-Tagging;
- Redaction Assistant;
- Community Request;
- Axon Standards;
- API integrations and other software capabilities.

The 2024 Axon agreement alone provided 126 Axon Records licenses, 126 Unlimited Auto-Transcribe licenses and 126 Respond Plus licenses, together with Evidence, Axon Air, API integrations and numerous additional products.

Once the hardware, accounts, cloud storage, APIs and user infrastructure are already in place, a materially new capability may no longer require the kind of visible hardware purchase that traditionally alerts the public to a new surveillance system.

The question therefore cannot be limited to what Bend owns today.

It must also include what existing systems can be configured or authorized to do tomorrow.

2. Bend has already experienced the difference between policy and configuration

Bend’s former Flock Safety ALPR program provides the clearest local example.

During approximately the first three weeks of Bend’s 2025 Flock pilot, federal immigration agencies accessed Bend Police camera data 279 times.

Bend Police had not intended to provide that access.

According to police officials, a Flock “Lookup” setting remained at its factory-default National setting rather than being restricted to State or Local access.

One configuration setting produced a surveillance outcome that differed dramatically from what local policy intended.

The City ultimately shut off the stationary Flock cameras.

Calling a technology responsible does not make its configuration responsible.

A written policy saying data should not be used in a particular way cannot substitute for technical controls, auditing, access restrictions and independent oversight capable of ensuring that the policy is actually followed.

3. Draft One demonstrates how an existing platform can acquire a fundamentally new function

Bend’s adoption of Axon Draft One illustrates a different oversight problem.

Bend originally acquired body-camera systems capable of recording police encounters. Its Axon ecosystem subsequently included Auto-Transcribe, which converts body-camera audio into text.

Draft One adds another layer:

Body-camera audio → automated transcript → generative AI → draft police narrative → officer-reviewed official report

That is not merely an improvement to a camera.

It is a new governmental function built from information collected by the existing system.

The distinction is especially important because Bend’s 2024 Axon agreement included Axon Records and Unlimited Auto-Transcribe, but the contract reviewed by Bend Privacy Alliance does not name Draft One.

The public presentation of that agreement focused primarily on consolidating existing Axon products, administrative efficiency and cost savings. Yet the underlying agreement contained a considerably broader collection of software products and integration capabilities.

This does not establish that the Council was misled.

It demonstrates something more fundamental:

A public discussion framed around a procurement can communicate far less about future technological capability than the underlying platform actually makes possible.

Draft One is therefore an important case study for the proposed legislative principle.

A City can move from recording an event, to transcribing it, to using artificial intelligence to help create the official government narrative of that event—without purchasing a new body camera.

4. Modern surveillance capability often expands through software rather than new hardware

Traditional public oversight frequently assumes that new surveillance capability arrives with a new object:

- A new camera.
- A new drone.
- A new sensor.
- A new contract.

That assumption increasingly fails with integrated public-safety platforms.

Capabilities may instead change through:

- software activation;
- subscription tiers;
- new licenses;
- API connections;
- interoperability between existing systems;
- vendor updates;
- new analytic tools;
- changed retention or sharing settings;
- administrative configuration;
- pilot programs or promotional access; or
- changes to the law governing what an existing system is allowed to do.

“Expanding allowed uses” can itself be a form of surveillance expansion even when Bend purchases no new hardware.

If Oregon law currently limits a particular search, retention period, data use, automated analysis or information-sharing practice, changing that law can increase the power of equipment already operating in Bend.

That is why the wording of Bend’s legislative priorities matters.

5. Axon’s patent portfolio shows why policy must anticipate capability growth

Bend Privacy Alliance has reviewed a substantial portion of Axon’s patent portfolio.

Those patents describe technologies involving areas such as:

- automated license plate recognition;
- geofencing and location-triggered camera behavior;
- multi-camera and cross-system interactions;
- real-time video and information integration;
- automated evidence processing;
- semantic and automated redaction;
- camera-field-of-view analysis;
- predictive identification of potentially relevant video sources; and
- other forms of automated processing within connected public-safety systems.

Bend Privacy Alliance is not claiming that Bend currently uses every capability described in those patents.

The distinction is important.

A patent establishes that a capability has been contemplated, developed or protected by the vendor. It does not prove that a particular Bend system is configured to perform it.

But the patent record is highly relevant to long-term governance.

It demonstrates that the technological platform Bend is buying into is not static.

The capabilities available during the life of a multi-year contract may be substantially different from those discussed when the contract was originally approved.

Public policy therefore should not assume that today's configuration defines tomorrow's surveillance capacity.

6. The national record shows that misuse is not merely theoretical

Bend's experience is enough to justify caution on its own.

But it does not exist in isolation.

The source archive maintained by Bend Privacy Alliance contains repeated documented examples from around the country involving misuse of ALPR databases, unauthorized searches, inappropriate data sharing, inadequate access controls and communities reconsidering surveillance programs after discovering how the systems were actually being used.

Recent incidents include law-enforcement personnel disciplined or terminated after unauthorized Flock searches involving spouses, acquaintances and other individuals.

These examples do not prove that Bend officers will misuse Bend systems.

They establish something different:

Access controls, audit mechanisms and enforceable restrictions are necessary precisely because public policy should not depend upon every authorized user always exercising perfect judgment.

Responsible governance assumes that mistakes, misuse, changing administrations and changing institutional priorities are possible.

Safeguards exist for those circumstances.

7. "Responsible" is a conclusion, not a standard

The proposed City language does not define:

- what technologies qualify as responsible;
- who makes that determination;
- whether privacy must be considered;
- whether civil-rights impacts must be examined;
- whether effectiveness must be independently demonstrated;
- whether new data-sharing authority is permitted;
- whether biometric technologies are included;
- whether artificial intelligence is included;
- whether surveillance systems must receive public review;
- whether the City's lobbyists may support legislation weakening existing restrictions; or
- whether Council must approve a particular expansion before the City advocates for it.

Without those answers, the adjective "responsible" supplies almost no enforceable limitation.

A vendor may describe a product as responsible.

A police department may believe a deployment is responsible.

A lobbyist may believe proposed legislation enables responsible technology.

A future City administration may interpret the term differently from the present Council.

None of those interpretations creates a meaningful boundary.

8. Bend should not decide in advance that expansion is the desired outcome

The most concerning words in the proposed principle are not “responsible technologies.”

They are:

“support expanding allowed uses.”

Those words establish the policy outcome before the particular issue has been presented.

A better process would ask:

- What technology is involved?
- What capability is currently prohibited or restricted?
- Why does Bend believe that restriction should change?
- What problem would expansion solve?
- What information would be collected, searched, analyzed or shared?
- What other systems could receive that information?
- What are the privacy and civil-rights consequences?
- What safeguards would be legally enforceable?
- What would the technology cost?
- How would the public know if its use subsequently expanded?

Only after those questions are answered should the City decide whether expanded authority is justified.

Conclusion

Bend has already seen surveillance capability change through configuration.

It has already assembled a public-safety platform in which cameras, ALPR, drones, evidence, records, transcription, real-time information and other systems can interact.

It has already adopted a generative-AI reporting capability that was not named in the major Axon agreement Bend Privacy Alliance reviewed.

And Bend’s principal public-safety technology vendor continues developing capabilities that extend well beyond the configurations presently documented in Bend.

Against that record, the City should not adopt a legislative principle instructing taxpayer-funded representatives to “support expanding allowed uses” of an undefined category of technology.

Bend Privacy Alliance is asking for a different order of operations:

- Identify the technology.
- Identify the proposed authority.
- Identify the risks.
- Establish the safeguards.
- Hold the public discussion.
- Then decide whether expansion is justified.

“Responsible technology” should be the conclusion reached after that process.

It should not be the phrase used to avoid it.