



17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

September 1, 2026

Legislative Research Commission
Capitol Annex Rm. 111
702 Capitol Ave.
Frankfort, KY, 40601-3448

Chairmen and Members of the Committee:

Thank you for the opportunity to submit written testimony on the use of automated license plate recognition (“ALPR”) technology. Axon Enterprise, Inc. (“Axon”) is a public safety technology company that, among other products, manufactures and supports ALPR camera systems used by law enforcement agencies nationwide. We appreciate the Committee’s attention to this issue as it considers how ALPR technology should be governed in Kentucky.

For more than 30 years, Axon has built products that protect life and promote truth and transparency. As new technologies emerge, we know that public safety agencies and community members require solutions that protect data and privacy. This is a responsibility we have carried since bringing body cameras to market in 2009. In line with our Responsible Innovation Framework, we will continue to invest in safeguards to help our customers meet or exceed the expectations of the communities they serve.

This testimony is intended to help the Committee understand how Axon’s ALPR technology functions, how the data it generates is collected, stored, and used, and how our system is designed from the ground up to support agency ownership and oversight.

How Axon’s ALPR Technology Works

Through Axon’s ALPR platforms, a high-speed camera captures an image of a passing vehicle and its plate. Onboard processing at the edge of the device extracts the plate characters and state of issuance, while the associated imagery is processed and stored securely once it reaches the cloud. The extracted plate is compared, in real time, against one or more “hotlists,” such as the National Crime Information Center (NCIC) database or an agency’s own list of plates tied to open investigations.

If a plate matches a hotlist entry, the system surfaces an alert for a human user to review. It does not take any automated enforcement action. Personnel evaluate the alert, apply judgment, and determine whether department policy and applicable law support any further action, such as a traffic stop. Detection is automated; the operational decision remains human.

ALPR reads license plates, not faces. It is not facial recognition technology and is not used to identify drivers, passengers, or other individuals, or to build a profile of a person’s movements.

How License Plate Data Is Collected, Stored, and Used

What data is captured

Each ALPR read associates a plate number and state of issuance with an image of the vehicle and plate, along with information about when and where the camera captured it. Axon’s cameras do not capture or process facial images or other information used to identify a driver or passenger.



17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

Who owns the data

Axon's ALPR products are built around an agency-controlled model. The law enforcement agency that deploys the camera owns and controls the data it collects: data stays within that agency's own environment at all times, visibility does not change unless the agency takes an explicit action, and sharing is deliberately configured, revocable, and prevented by design from occurring without that action. Axon does not own, sell, resell, or independently use agency ALPR data for any other purpose, including marketing, unrelated analysis, or product development, without the agency's separate written consent. Axon acts as a processor and custodian of the data on the agency's behalf, and the agency remains the decision-maker on retention, access, sharing, and disclosure. The one narrow, fully optional exception is Axon's Customer Experience Improvement Program, which an agency may join to help improve the technology and may leave at any time; full plate reads are not used even for that purpose.

Where and how data is stored

Data captured by Axon ALPR cameras is transmitted over encrypted connections and stored in U.S. government cloud regions the agency selects, within that agency's own logically isolated environment, not pooled together with other agencies' data. Data is encrypted both in transit and at rest using industry-standard AES-256 encryption, and access is governed by role-based permissions with single sign-on and multi-factor authentication that the agency configures. Axon's systems are independently validated against security standards including SOC 2 Type II, ISO 27001, ISO 27701, FedRAMP High, and the FBI's CJIS Security Policy. Axon has no standing access to agency data; any Axon access is limited to specific, agency-initiated support requests, and that access is itself temporary, logged, and auditable by the agency.

Retention and deletion

Retention periods are set by the agency, not fixed by Axon, and an agency can configure separate, shorter retention for reads that never match a hotlist and longer retention for reads connected to an open case. Non-evidentiary reads are purged automatically once the retention window closes, and every deletion, like every other action taken on the data, is written to an immutable audit log that the agency can review at any time. The agency configures and controls the settings.

How data is used

Before returning results, Axon's system requires the user to enter a reason for the search and to select an authorized offense category. Searches outside an agency's permitted categories simply return no data. This means every use of the system carries a documented, reviewable purpose tied to a named user, rather than an open-ended lookup capability.

Data Sharing, Access, and Oversight

Because sharing of ALPR data across jurisdictions has drawn significant public attention, we want to be direct with the Committee about how Axon's system is designed to handle it.

- Sharing between agencies is off by default. It is not automatic and does not happen without an agency's affirmative action.
- Where an agency chooses to share, sharing is invite-only and requires mutual consent: the owning agency invites a specific partner, and that partner must separately review and accept before any data becomes visible to it.
- Shared access does not create a copy of the data. The receiving agency queries the owning agency's data in place, cannot re-share what it accessed, and the owning agency can revoke that access at any time.



17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

- New sharing relationships default to their most limited setting, exposing only reads that match the receiving agency's own hotlist, and every cross-agency search still requires a declared offense category, with data outside the donor's permitted categories excluded from results.
- There is no national pool of ALPR data operated by Axon, and no standing or automatic access for federal agencies. Federal and enterprise accounts are excluded from ALPR sharing entirely. Any request from a federal agency, like any other outside request, must be directed to the owning agency, and Axon does not independently disclose agency data in response to such requests.
- Subpoenas, warrants, and public records requests directed to Axon are routed to the owning agency as the data owner, and the agency, not Axon, determines how to respond under applicable law and its own policy. Like any custodian of records, Axon must comply with a valid, legally binding court order directed to Axon itself, but where legally permitted, Axon notifies the agency first so it has the opportunity to object.

Every access to ALPR data, every configuration change, and every sharing decision is written to an immutable audit log capturing the user, the action, the time, and, when configured, the stated reason. Agencies can review this log at any time and can generate reports for internal affairs, supervisory review, or public records requests, with the ability to redact personally identifying information such as officer name, plate number, or case number before external release.

Agencies also have access to an optional ALPR Policy and Usage Transparency Portal, which an agency can configure to publish its retention policy, usage metrics, and program details to the public, and which can also disclose active sharing relationships so a community can see not just how ALPR data is used but with whom it is being shared. A one-button ALPR audit report is likewise available for supervisory review, internal affairs, and public disclosure, with the ability to redact personally identifying details before external release. We encourage agencies deploying this technology to make use of these tools.

Conclusion

Axon's approach to safeguarding public safety data, including a Responsible Innovation Framework that embeds data ownership, usage controls, and transparent governance directly into our products, has been built through decades of collaboration with the agencies and communities we serve. Axon appreciates the Committee's attention to ALPR technology, and we are committed to supporting agencies in Kentucky in deploying this technology responsibly.

Sincerely,

Sincerely,

A handwritten signature in black ink that reads 'Isaiah Fields'.

Isaiah Fields
Chief Legal Officer
Axon