OHIO LEGISLATIVE SERVICE COMMISSION

www.lsc.ohio.gov

Office of Research and Drafting

Legislative Budget Office

S.B. 469
136th General Assembly

Bill Analysis

Version: As Introduced

Primary Sponsor: Sen. Cutrona

Larry Gunter, Jr., Research Analyst

SUMMARY

- Generally prohibits a government entity from doing any of the following:
  - Selling to, transferring to, or sharing with a private person any captured surveillance data that was collected from an automated license plate recognition system (ALPRS) or mass surveillance technology;
  - Transferring or sharing with any other government entity any captured surveillance data that was collected from either an ALPRS or mass surveillance technology without a warrant; and
  - Operating an ALPRS or mass surveillance technology within 500 feet of a place of worship or a firearms retailer.
- Imposes retention restrictions on a government entity that collects or receives captured surveillance data.
- Creates limited exemptions to those prohibitions for toll collection on the Ohio Turnpike or other toll roads and traffic law photo-monitoring devices (i.e., red light and speed traffic cameras).
- Authorizes the Attorney General to bring an action for a temporary restraining order, preliminary injunction, or permanent injunction to restrain prohibited acts or practices.
- Authorizes an individual to commence a civil cause of action against a government entity that unlawfully used an ALPRS or mass surveillance technology.
- Requires a government entity using ALPRS, mass surveillance technology, or captured surveillance data to do all the following:
  - Adopt policies concerning its ethical use;
  - Conduct monthly internal audits; and

- Annually report its use and practices to the Attorney General.

- Exempts images and data captured by an ALPRS, regardless of where the data is maintained, and images and data captured by other mass surveillance technology from the Public Records Law.

DETAILED ANALYSIS

Overview

The bill establishes multiple prohibitions regarding the use of captured surveillance data obtained from an automated license plate recognition system (ALPRS) or mass surveillance technology. An ALPRS is a system of one or more mobile or fixed high-speed cameras, sensors, or devices, combined with computer algorithms, that can convert images of license plates, vehicle location, or other vehicle identification markers into computer-readable data. ALPRS generally are attached to law enforcement vehicles and infrastructure, such as highway overpasses, street poles, and bridges. Many local governments have entered into contracts with the ALPRS manufacturing company, Flock Safety, to lease, purchase, install, or operate an ALPRS. Although other companies besides Flock Safety manufacture these systems, ALPRS have become commonly referred to as "flock cameras."

Mass surveillance technology is any technology or device designed primarily to monitor, record, capture, or analyze the movements, activities, associations, or identifying characteristics of an individual in public spaces. Mass surveillance technology includes cameras, sensors, biometric identification systems, facial recognition systems, and gait recognition systems. However, it does not include a camera that is used solely for monitoring a specific and defined area for immediate security purposes if that camera is not integrated with an identification or recognition database or analytics system.

Captured surveillance data is the data and metadata captured by, derived from, generated by, or inferred from an ALPRS or mass surveillance technology, including photographs, videos, location information, or other forms of observation recording.[1]

Prohibited uses of surveillance data by government entities

The bill restricts the collection and use of captured surveillance data by a government entity, which is a state agency, public institution, political subdivision, or any other organized body, office, agency, institution, or entity established by the laws of this state for the exercise of any function of government.[2]

Specifically, it prohibits a government entity and its agents and employees from knowingly doing any of the following:[3]

[1] R.C. 5507.01(A), (B), and (F).

[2] R.C. 5507.01(D).

[3] R.C. 5507.02(A)(2), (A)(3), and (D).

1. Selling to, transferring to, or sharing with a private person[4] any captured surveillance data;
2. Transferring or sharing with any other government entity any captured surveillance data unless the other government entity obtains a search warrant for the data; and
3. Operating an ALPRS or mass surveillance technology within 500 feet of either of the following:
    a. Any place of worship, which is a building where activities of an organized religious group are conducted, including the grounds and any other buildings on the grounds used for such activities;[5] or
    b. Any firearms retailer, which is a physical place of business in Ohio that is engaged in the lawful selling or trading of firearms, antique firearms, or ammunition to be used in firearms or antique firearms.[6]

The bill imposes a fourth degree felony on a person who violates any of the above prohibitions.[7]

Retention

In addition to the prohibitions governing the collection, sharing, and use of captured surveillance data, the bill imposes retention restrictions on a government entity that collects or receives captured surveillance data.

Specifically, the bill prohibits a government entity and its agents and employees from knowingly retaining captured surveillance data for more than ten days after it was: (1) collected, or (2) received from another government entity under a search warrant. Additionally, within 11 days after receiving or collecting captured surveillance data, it also requires a government entity or its employees or agents to permanently delete and destroy such data in its control that was captured after the bill's effective date. However, these requirements do not apply to captured surveillance data that is any of the following:

- Relevant to an ongoing trial, litigation, or other legal proceeding until it is determined that such data is no longer necessary for that purpose;
- Prohibited from being deleted or destroyed by either federal law, state law, or a court order; or

[4] Under R.C. 5507.01(H), a private person is an individual, corporation, business trust, estate, trust, partnership, unincorporated association, limited liability company, two or more of any of the foregoing having a joint or common interest, or any other legal or commercial entity. However, a private person is not an individual who is employed by or contracted with a government entity while the individual is acting in an official capacity on behalf of a government entity.

[5] R.C. 5507.01(I) and see R.C. 5104.01(MM), not in the bill.

[6] R.C. 5507.01(C).

[7] R.C. 5507.99.

- Obtained or retained pursuant to a valid search warrant.[8]

A government entity or a government entity's agent or employee that violates the retention prohibition is guilty of a fourth degree felony.[9]

Exemptions

The bill's prohibitions do not apply to the Ohio Turnpike and Infrastructure Commission or other toll project operators operating a camera for toll collection on a turnpike project, toll road, or toll bridge and any captured surveillance data that originates from that camera so long as the camera and data:

- Are used solely to bill users of that toll road or bridge by an electronic toll collection system or other similar means;
- Comply with applicable statutory requirements regarding motor vehicle owner and registration information collection and confidentiality for that information; and
- Are not integrated with a law enforcement database or accessible to law enforcement without a warrant.

These prohibitions also do not apply to traffic law photo-monitoring devices (i.e., red light and speed traffic cameras) that are operated in accordance with state or local laws.[10]

The bill explicitly states that it does not prohibit a private person from willingly sharing captured surveillance data with a law enforcement agency or its agents or employees.[11]

Attorney General enforcement

If the Attorney General, by the Attorney General's own inquiries or investigations or as a result of complaints, has reasonable cause to believe that any person has engaged or is engaging in an act or practice that violates the bill's prohibitions, the bill authorizes the Attorney General to bring an action, with proper notice,[12] for a temporary restraining order (TRO), preliminary injunction, or permanent injunction to restrain the act or practice. A court may issue a TRO, preliminary injunction, or permanent injunction to restrain and prevent the act or practice if the Attorney General shows, by a preponderance of the evidence, that the person has violated the bill's prohibitions.[13]

---

[8] R.C. 5507.02(A)(1), (B), and (C).

[9] R.C. 5507.99.

[10] R.C. 5507.02(E).

[11] R.C. 5507.02(F).

[12] Civ. R. 65.

[13] R.C. 5507.04.

Private civil action

The bill authorizes an individual, either alone or as a party to a class action, to commence a civil cause of action against a government entity that utilized an ALPRS or a mass surveillance technology if one of the following apply:

1. The individual's captured surveillance data was sold, transferred, or shared in violation of the bill's prohibition; or
2. The individual's movements, activities, or vehicle were monitored, recorded, captured, or analyzed by an ALPRS or a mass surveillance technology in violation of the bill's prohibition.

A prevailing plaintiff is entitled to reasonable attorney's fees, the costs of bringing the civil action, and all the following, as applicable:

1. An injunction or a TRO prohibiting further use of the ALPRS or mass surveillance technology or destruction of all captured surveillance data;
2. Compensatory damages, including actual damages, for harm resulting from the violation;
3. Punitive damages for harm resulting from the violation; and
4. Any other relief the court determines is just and proper.

The bill explicitly states that sovereign immunity, qualified immunity, or governmental immunity are not defenses to any action brought under the individual's claim. It also voids, from the outset, any contractual provision, arbitration clause, choice of law provision, or forum selection clause that purports to limit, waive, or restrict the rights or remedies authorized by the bill's provisions governing private causes of actions.[14]

Policies, audits, and reporting

Policies

The bill requires any government entity that uses an ALPRS, mass surveillance technology, or collects captured surveillance data to adopt a policy governing the entity's ethical use of those technologies and data, as applicable. The policy must ensure that access of any captured surveillance data is granted only to chiefs of police, village marshals, county sheriffs, county prosecuting attorneys, or other designees within the government entity who act in a supervisory role or who otherwise provide oversight and direction for personnel. The policy also must require the tracking of each person who accesses, reviews, or uses the captured surveillance data each time that the data is accessed, reviewed, or otherwise used.[15]

Audits

Additionally, the bill requires a government entity to conduct a monthly internal audit of its use of ALPRS, mass surveillance technology, and captured surveillance data, as applicable. The

[14] R.C. 5507.03.

[15] R.C. 5507.05(A)(1).

government entity must develop standards and practices for conducting monthly internal audits of the entity's use of ALPRS, mass surveillance technology, and captured surveillance data to ensure the entity complies with all applicable laws.[16]

Reports

The bill requires a government entity to annually report to the Attorney General its practices and usage of ALPRS, mass surveillance technology, and captured surveillance data. In that report, the government entity must include all of the following:

1. The number of license plates scanned, as applicable;
2. The number of instances in which the captured surveillance data resulted in arrest, citation, prosecution, or a combination thereof;
3. The number of times captured surveillance data was shared with or accessed by another government entity, even if that data was shared inadvertently or by mistake and such sharing was discovered after the fact;
4. The number of times captured surveillance data was shared or accessed pursuant to a judicial warrant or used in court proceedings;
5. Any changes in policies adopted by a government entity that has or may have an effect on the privacy concerns of private persons; and
6. The results of the internal audits from the prior 12 months.

A government entity must compile and submit the annual report to the Attorney General by January 1 each year. By April 1 each year, the Attorney General must submit a consolidated summary of the reports it receives from each government entity to the Speaker of the House, the Senate President, and the minority leaders of both the House and Senate.

A government entity must conspicuously post both of the following on its website:

1. Each annual report submitted to the Attorney General; and
2. Any policy adopted governing the entity's ethical use of ALPRS, mass surveillance technology, and captured surveillance data.[17]

Public records exemption

Under current law, images and data captured by an ALPRS and maintained in a law enforcement database are not considered public records and thus are exempted from the Public Records Law. The bill broadens this exemption by (1) applying it to all ALPRS-captured images and data, regardless of where they are maintained, and (2) extending it to images and data captured by other mass surveillance technologies.[18]

---

[16] R.C. 5507.05(A)(2) and (3).

[17] R.C. 5507.05(A)(4), (B), (C), and (D).

[18] R.C. 149.43(yy).

HISTORY

Action	Date
Introduced	09-14-26

ANSB0469IN-136/ar