OHIO LEGISLATIVE SERVICE COMMISSION

www.lsc.ohio.gov

Office of Research and Drafting

Legislative Budget Office

H.B. 1009
136th General Assembly

Bill Analysis

Version: As Introduced

Primary Sponsors: Reps. Newman and Willis

Racheal Vargo, Research Analyst

SUMMARY

- Prohibits a private person from knowingly accessing, collecting, using, selling, transferring, or sharing any captured surveillance data and establishes a criminal penalty for violating that prohibition.
- Prohibits a government entity from knowingly accessing, collecting, using, selling, transferring, or sharing any captured surveillance data.
- Prohibits a peace officer from knowingly accessing, collecting, using, transferring, or sharing any captured surveillance data beyond the scope of the officer's duties and establishes a criminal penalty for violating that prohibition.
- Establishes exemptions for certain uses of captured surveillance data.

DETAILED ANALYSIS

Overview of the Stop Flock Abuse Act

The bill regulates the use of automated license plate recognition systems (ALPRS) and mass surveillance technology. It also establishes various prohibitions regarding the use of captured surveillance data obtained from an 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 is capable of converting images of license plates, vehicle location, or other vehicle identification markers into computer-readable data. ALPRS 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." Accordingly, the bill is named the "Stop Flock Abuse Act."[1]

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 ALRPS or mass surveillance technology, including photographs, videos, location information, or other forms of observation recording.[2]

Prohibitions against the use of captured surveillance data

The bill prohibits a private person from knowingly accessing, collecting, using, selling, transferring, or sharing any captured surveillance data. 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. A private person does not include an individual employed by or contracted with a government entity while that individual is acting in an official capacity on behalf of a government entity. Whoever violates that prohibition is guilty of a fifth degree felony.[3]

Similarly, the bill also prohibits a government entity from knowingly accessing, collecting, using, selling, transferring, or sharing any captured surveillance data. A government entity is a state agency, public institution, policial subdivision, or any other organized body, office, agency, institution, or entity established by Ohio law to exercise any government function.[4]

Additionally, the bill prohibits a peace officer from knowingly accessing, collecting, using, transferring, or sharing any captured surveillance data beyond the scope of the officer's duties. A peace officer includes the Superintendent and troopers of the Ohio State Highway Patrol. Whoever violates that prohibition is guilty of a fifth degree felony.[5]

Exemptions

The bill's prohibitions do not apply to any of the following:

[1] Section 2.

[2] R.C. 5507.01(A), (B), and (E).

[3] R.C. 5507.01(G), 5507.02(A), and 5507.99.

[4] R.C. 5507.01(C) and 5507.02(B).

[5] R.C. 5507.01(F), 5507.02(D), 5507.99, and see 109.71, not in the bill, for the definition of peace officer.

- A law enforcement agency (a government entity that employs peace officers to perform law enforcement duties)[6] or peace officer accessing, collecting, using, transferring, or sharing captured surveillance data in the course of law enforcement activities;
- A traffic law photo-monitoring device that is operated in accordance with state law or a substantially equivalent municipal ordinance;
- A private person or government entity accessing, collecting, using, transferring, or sharing captured surveillance data in any of the following ways:
  - In the course of normal business activity and within the scope of the person's normal duties and employment or a government entity's normal activities, including for insurance purposes or for regulating access to private property; or
  - In accordance with a warrant, a court order, or any other similar circumstance authorized by law.
- The Ohio Turnpike and Infrastructure Commission or other toll project operator 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 if 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 regarding that information; and
  - Are not integrated with a law enforcement database or accessible to law enforcement without a warrant.[7]

HISTORY

Action	Date
Introduced	09-14-26

ANHB1009IN-136/ts

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

[7] R.C. 5507.02(C).