THE AUTOMATED LICENSE PLATE SURVEILLANCE CONSENT AND ACCOUNTABILITY ACT

Model legislation drafted by The Existentialist Republic. Bracketed text marks the items a sponsor adapts to state code.

AN ACT relating to public consent requirements for automated license plate recognition systems; establishing criminal penalties for unauthorized deployment; establishing civil penalties for vendors; creating a private right of action; and prescribing data protection requirements.

SECTION 1. SHORT TITLE.

This act may be cited as the Automated License Plate Surveillance Consent and Accountability Act.

SECTION 2. LEGISLATIVE FINDINGS.

The legislature finds that:

(a) Automated license plate recognition systems record the location, direction of travel, date, and time of every vehicle that passes them and retain that information in searchable databases, creating a record of the movements of persons who are suspected of no crime.

(b) A single private vendor operates more than 100,000 such cameras in the United States and processes approximately 20 billion plate scans per month across a shared national network.

(c) Governing bodies in multiple states have discovered, through audits and investigative reporting, that data collected in their jurisdictions was searched by or transferred to federal agencies and out-of-state agencies without local authorization, including thousands of immigration-related searches conducted through local law enforcement accounts.

(d) One municipality discovered roughly 600,000 searches of its data in a single year by more than 250 agencies it had never approved, and litigation in another state alleges that out-of-state and federal agencies searched one city's data more than 1.6 million times in seven months.

(e) Vendors of these systems have installed cameras without required permits, made false statements to governing bodies concerning system capabilities and data sharing, reinstalled cameras after being ordered to remove them, and revised standard contract terms to restrict the ability of governing bodies to terminate.

(f) Deployment decisions are frequently made without public notice, without a recorded vote, and through no-cost trial programs that receive no procurement review, so residents learn that the systems exist only after they are operating.

(g) Existing law in this state and others regulates the use and retention of data after collection but attaches no personal consequence to the decision to deploy such systems without public consent.

(h) Federal law, 18 U.S.C. § 2511, classifies the unauthorized interception of a single wire communication as a felony punishable by imprisonment for up to five years. A system that records the movements of every vehicle in a jurisdiction warrants penalties graded at or above that standard.

(i) Public consent, obtained through noticed hearings and a recorded vote of elected representatives, is the minimum lawful condition for the operation of mass surveillance systems in a free state.

SECTION 3. DEFINITIONS.

As used in this act:

(a) "Automated license plate recognition system" or "ALPR system" means one or more cameras, together with associated hardware, software, or services, that automatically capture images of license plates, vehicles, or vehicle characteristics and convert them into machine-readable or searchable data. The term includes systems provided as a service and access to any shared or networked database of such data.

(b) "Deploy" means to install, activate, operate, connect to a shared data network, or obtain ongoing access to data from an ALPR system.

(c) "Authorizing ordinance" means an ordinance or resolution adopted by recorded vote of the governing body of the jurisdiction after no fewer than two public hearings, each noticed at least 30 days in advance in accordance with [cite state open meetings law], where the published notice and agenda materials for each hearing include: the number of cameras and their locations or location criteria; the identity of the vendor and the complete contract, including cost; the categories of data to be collected; the retention period; every entity that will have access to the data or the network; and the audit provisions.

(d) "Governing body" means the elected legislative body of a county, city, town, or other political subdivision, or, for a state agency, [the legislature].

(e) "Public officer or public employee" means any elected official, appointed official, or employee of the state or a political subdivision.

(f) "Vendor" means any person or entity that sells, leases, donates, installs, operates, or provides an ALPR system or access to ALPR data as a service.

(g) "No-cost deployment" means any deployment provided as a trial, pilot, demonstration, grant-funded program, or donation, or otherwise without expenditure of public funds.

(h) "Plate capture" means each instance in which an ALPR system records a license plate, vehicle image, or vehicle characteristic and converts it into data.

(i) "Judicial warrant" means a warrant issued by a judge or magistrate of a court of competent jurisdiction upon a finding of probable cause. The term does not include an administrative warrant, an agency subpoena, an administrative subpoena, a civil investigative demand, or any authorization issued by an agency for its own use.

SECTION 4. PUBLIC CONSENT REQUIRED.

(1) No agency of the state or of a political subdivision may deploy an ALPR system without an authorizing ordinance.

(2) A material change to an authorized deployment, including any new data-sharing recipient, any new system capability, any increase in the number of cameras, or any amendment to the vendor contract, requires a new authorizing ordinance adopted by the same procedure.

(3) An authorizing ordinance expires two years after adoption unless renewed by the same procedure, following publication of a report stating the number of plate captures, every search performed, and every entity that accessed the data during the authorization period.

(4) The complete vendor contract, the system's data-sharing configuration, and all audit logs are public records and are not exempt from disclosure as trade secrets or proprietary information.

SECTION 5. CRIMINAL PENALTY FOR UNAUTHORIZED DEPLOYMENT.

(1) A public officer or public employee who knowingly deploys, installs, authorizes, or executes a contract or agreement for an ALPR system, including any no-cost deployment, without an authorizing ordinance is guilty of a felony punishable by imprisonment for up to five years, a fine of up to $10,000, or both [insert corresponding state felony classification].

(2) The offense is a felony punishable by imprisonment for up to ten years, a fine of up to $20,000, or both [insert corresponding state felony classification], if the officer or employee:

(a) concealed the deployment from the governing body or the public;

(b) made a false or misleading statement to the governing body or the public regarding the system's existence, capabilities, data collection, or data sharing; or

(c) continued operation of the system more than 30 days after receiving written notice of noncompliance from the attorney general, the governing body, or a court.

(3) The attorney general has concurrent original jurisdiction to investigate and prosecute violations of this section.

(4) Conviction under this section constitutes malfeasance in office. The office or position is forfeited upon conviction, and the person is disqualified from holding public office in this state

for ten years.

(5) No public funds and no insurance purchased with public funds may be used to pay a fine imposed under this section or to indemnify a person convicted under this section.

(6) It is not a defense to a prosecution under this section that the system was provided at no cost or that no public funds were expended.

SECTION 6. VENDOR DUTIES AND CIVIL PENALTIES.

(1) A vendor shall not install or activate an ALPR system for an agency of this state or a political subdivision, and shall not connect any such agency to a shared data network, before receiving a certified copy of the authorizing ordinance. This duty applies regardless of the vendor's knowledge or intent.

(2) A vendor that violates subsection (1), or that operates a system after the authorization expires or is revoked, is liable to each person whose vehicle was recorded during the unauthorized period for statutory damages of $1,000 per plate capture, or $5,000 per plate capture if the violation was willful or reckless.

(3) A vendor in violation is additionally liable to the state for a civil penalty of $10,000 per camera per day of unauthorized operation.

(4) Within 30 days of receiving notice of a violation, the vendor shall permanently delete all data collected during the unauthorized period and file a sworn certification of deletion signed by an officer of the company. Failure to do so incurs an additional civil penalty of $10,000 per day.

(5) A vendor found in violation of this section is barred from entering into any contract with this state or any of its political subdivisions for five years.

(6) Any contract for an unauthorized deployment is void and unenforceable. Any contract provision that restricts a governing body's ability to terminate when it declines to approve or fund a deployment is void. Any provision requiring arbitration of claims arising under this act is unenforceable.

SECTION 7. DATA PROTECTION REQUIREMENTS FOR AUTHORIZED SYSTEMS.

(1) No ALPR data collected in this state may be shared with, transferred to, or made searchable by any federal agency or any out-of-state entity except pursuant to a judicial warrant.

(2) No ALPR system or its data may be used for immigration investigation or enforcement; for the surveillance of reproductive health care facilities, gender-affirming health care facilities, or persons seeking or providing such care; for the surveillance of activity protected by the First Amendment; or for any personal purpose of an officer or employee, including locating or monitoring a person with whom the officer or employee has a personal relationship.

(3) ALPR data shall be permanently deleted no later than 30 days after collection unless it is retained as evidence in a specific investigation pursuant to a judicial warrant.

(4) Every search of ALPR data shall be logged with the identity of the person searching, the date and time, and the stated purpose. Audit logs are public records, with plate numbers redacted.

(5) A willful violation of this section is a felony punishable by imprisonment for up to five years, a fine of up to $10,000, or both [insert corresponding state felony classification], and gives rise to the remedies in Section 6(2) and Section 8.

SECTION 8. PRIVATE RIGHT OF ACTION.

(1) Any person whose vehicle was recorded in violation of this act may bring a civil action for the statutory damages provided in Section 6, together with injunctive and declaratory relief.

(2) Any resident of a jurisdiction in which a violation occurs may bring a civil action for injunctive and declaratory relief.

(3) A prevailing plaintiff shall recover reasonable attorney fees and costs.

(4) An action under this section must be commenced within three years of the date the violation was discovered or reasonably should have been discovered.

(5) No agreement to arbitrate applies to claims arising under this act.

SECTION 9. ATTORNEY GENERAL ENFORCEMENT.

The attorney general may bring civil actions to recover the penalties in Section 6, may seek injunctive relief, and has the concurrent criminal jurisdiction provided in Section 5(3).

SECTION 10. RELATION TO LOCAL LAW.

This act establishes minimum requirements. A political subdivision may adopt stricter requirements, including prohibiting ALPR systems entirely.

SECTION 11. EXISTING SYSTEMS.

(1) An agency operating an ALPR system on the effective date of this act has 180 days to obtain an authorizing ordinance under Section 4 or to cease operation and complete removal of the system within 30 additional days.

(2) Operation beyond the deadlines in subsection (1) constitutes unauthorized deployment for all purposes of Sections 5 and 6, and the unauthorized period runs from the deadline.

(3) Data collected before the effective date without an authorizing ordinance shall be permanently deleted within 60 days of the effective date unless retained as evidence pursuant to a judicial warrant.

SECTION 12. SEVERABILITY.

If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act and its application to other persons or circumstances are not affected.

SECTION 13. EFFECTIVE DATE.

This act takes effect [immediately / 90 days after adjournment].