

The Protecting Everyone from Excessive Police Surveillance (PEEPS) Act

Model Legislation
August 2025
Revised in September 2026

Section 1. Short Title.

This Act may be cited as the PEEPS Act.

Section 2. Legislative Findings and Purpose.

The legislature finds that government officials or government entities violate individuals' right to privacy, and the constitutional principles that protect it, when, without adequate safeguards, they use technology to create, access, or share data that reveal, or can be used to reveal, individuals' or vehicles' location information. This Act regulates the access to, sharing of, retention of, and security of that information.

Section 3. Definitions.

For purposes of this Act:

“Access” means viewing, querying, retrieving, copying, transmitting, analyzing, downloading, or otherwise using a database, whether manually or automatically.

“Collect” means using technology, including but not limited to license plate readers, cameras, sensors, or aerial drones, to record information about the physical locations, movements, or movement patterns of individuals or vehicles.

“Contemporaneous location information” means data that, when accessed, reveals the location or locations of individuals or vehicles less than two hours before the time of the access.

“Database” means a physical or digital information storage system, whether publicly or privately owned, that contains location information in any form, including but not limited to photographs, video, audio recordings, license plate data, facial recognition data, cell site location information, device signal data, or any combination, index, or analysis of these.

“Government entity” means any government agency, office, bureau, division, board, council, commission, or political subdivision.

“Government official” means any officer, employee, agent, contractor, or representative of a government entity.

“Historical location information” means data that, when accessed, reveals the locations of individuals or vehicles more than two hours before the time of the access.

“Hotlist” means a list of license plate numbers or other unique identifiers that is compared, automatically or manually, against contemporaneous location information as it is collected, for the purpose of generating an alert when a match occurs.

“Location information” means contemporaneous location information and historical location information. The term does not include:

- a. audio, video, or photographic recordings, including recordings captured by a camera in a government-owned building, a body-worn camera worn by an on-duty government official, or a dashboard camera installed in or on a vehicle owned by a government entity, that satisfy both of the following:
 1. the recordings have not been processed or indexed to identify, classify, match, reidentify, track, or reconstruct movements of a particular individual or vehicle, other than an on-duty government official or a government-owned vehicle; and
 2. the recordings have not been networked, pooled, combined, or otherwise organized with other recordings or data in a manner that readily permits a government official to search across multiple locations for an individual, vehicle, or group of individuals or vehicles or to reconstruct movements across those locations;
- b. information generated by a device worn or carried by an individual pursuant to a court order or a condition of pretrial release, probation, parole, or other individualized supervision;
- c. records created or maintained for administrative or recordkeeping purposes, rather than to track or reconstruct the movements of individuals or vehicles, including property, tax, vital, business- and professional-licensing, voter-registration, 9-1-1 and emergency-dispatch, and court records; and
- d. information that reveals only an address of residence, ownership, or registration, and not the presence of a particular individual or vehicle at a particular time.

“Supervisor” means a government official who has the authority to direct and discipline several government officials within a government entity.

“Warrant” means a court order that meets the requirements of the Fourth Amendment’s warrant clause. For purposes of this Act, a subpoena is not a warrant.

Section 4. Location Information Access.

- a. A government official may not access historical location information unless one or more of the following exceptions apply:
 1. the government official has obtained a warrant to access the database;
 2. each individual whose historical location information would be revealed expressly consents, so long as that consent does not allow the government official to access the historical location information of individuals who have not expressly consented;
 3. the registered owner of a vehicle reports the vehicle lost or stolen and expressly consents;
 4. exigent circumstances make it impractical to obtain a warrant before the exigency expires; or
 5. the government official is carrying out one or more of the following purposes and uses the historical location information solely for those purposes:
 - i. apprehending an individual for whom there is an outstanding arrest warrant, provided that the offense for which the warrant was issued would be a felony under the laws of this state;
 - ii. toll collection and enforcement, provided that the access is limited to a specific toll or fare transaction or violation and does not reveal the individual's or vehicle's location at any other time;
 - iii. traffic enforcement, provided that the access is limited to a specific traffic violation and does not reveal the individual's or vehicle's location at any other time;
 - iv. parking enforcement, provided that the access is limited to a specific parking violation and does not reveal the individual's or vehicle's location at any other time; or
 - v. information security, as necessary to implement the requirements of section 5.
- b. A government official may not access contemporaneous location information unless one or more of the following exceptions apply:
 1. an exception listed in subsection (a) applies, applied as though each reference in that subsection to historical location information were a reference to contemporaneous location information;

2. the government official has a reasonable suspicion that the individual or vehicle whose location would be revealed by the access has committed, is committing, or is about to commit an offense that would be a felony under the laws of this state;
3. the government official has an objectively reasonable basis to believe that the access is necessary to prevent imminent harm to a person or imminent substantial damage to property; or
4. the access consists solely of the comparison of contemporaneous location information against a hotlist and the receipt or review of any alert generated by that comparison, provided that the access is limited to the contemporaneous location information produced by the single collection that generated the alert.

Section 5. Location Information Security.

- a. A government official or government entity that collects location information may not share it outside the official's or entity's jurisdiction, except for a reason set forth in section 4 or pursuant to a valid court order. For purposes of this Act, a subpoena is not a valid court order.
- b. A government official or government entity that collects location information may not sell or convey it to a private, nongovernmental third party for any reason, whether as a market transaction, a response to a public records request, or otherwise. This subsection does not prohibit a government official or government entity from conveying location information to a vendor that operates the database on the official's or entity's behalf, solely as necessary for the vendor to correct errors or defects in, or to secure, the database, software system, or related technology.
- c. A government official or government entity that collects location information shall adopt a policy for compliance with this Act. The policy shall:
 1. ensure that the security and access requirements of this Act are being followed;
 2. ensure that location information is encrypted or otherwise rendered unreadable to an unauthorized person using methodology or technology generally accepted in the field of information security;
 3. ensure that government officials do not access a database that reveals location information absent a showing to a supervisor, and written approval by that supervisor, that the access complies with section 4(a);
 4. ensure that a record is created and maintained every time location information is accessed, which record shall include:
 - i. the identity of the government official and government entity;

- ii. the specific purpose for such access;
 - iii. the provision of section 4 that permitted access and information sufficient to verify that the provision was satisfied;
 - iv. the written supervisor approval that granted access; and
 - v. the description of the location information accessed;
- 5. ensure that the records required under paragraph (4) of this subsection are audited by one or more supervisors not less frequently than every 30 days to ensure compliance with this Act. The government official or government entity shall create written standardized policies or practices for those audits that require, at a minimum:
 - i. verification that all information required under paragraph (4) of this subsection has been provided;
 - ii. verification that the specific purpose for which access was sought complies with this Act;
 - iii. verification that the scope of the location information accessed was appropriate in light of the specific purpose, including where the access is pursuant to a warrant, verification that the scope of the location information accessed is consistent with what the warrant permits;
 - iv. evaluation of whether any other factors suggest noncompliance with this Act, such as large volumes of searches by the same official, differing reasons for searching for similar location information, repeat searches of the same individual's or vehicle's location information without a warrant, or any other factors that would tend to suggest that the specific purpose provided for the search was pretextual or not permitted under this Act; and
 - v. if a supervisor conducting the audit determines or has reason to believe that a government official or government entity has violated any provision of this Act, further investigation of that actual or suspected violation;
- 6. ensure the creation and maintenance of an annual report that both compiles and summarizes the records described in paragraph (4) of this subsection, which report shall be made available to the legislature and the Governor on written request and to individuals pursuant to a valid public records request, provided that, before making the report available under this paragraph, the government official or entity shall redact from the report all personally identifiable information, including but not limited to license plate numbers and facial images; and

7. ensure that all government officials whose duties include accessing a database that contains location information complete training on how to comply with this Act and the compliance policy adopted pursuant to this subsection. The training may not be created or administered by a private entity whose business involves collecting location information.

Section 6. Retention of Location Information.

- a. Except as provided in subsection (b), a government official or government entity that collects location information may not retain the information for more than seven days after the date the information is collected.
- b. Location information that was accessed in compliance with section 4 may be retained for more than seven days only if:
 1. a valid judicial warrant or valid court order expressly authorizes the government official or government entity to retain the location information for more than seven days;
 2. the information is necessary to preserve evidence in an active criminal investigation, a supervisor makes a written determination, based on specific and articulable facts, that retaining the historical location information for more than seven days is required to apply for or obtain a warrant, and the information is not retained later than the 14th day after the date the information is collected; or
 3. an individual expressly consents to the retention of the individual's location information for more than seven days, and the consent complies with the requirements of section 4(a)(2) or (3).
- c. If a government official or government entity does not obtain a warrant to preserve location information retained under paragraph (2) of subsection (b) before the expiration of the period described in that paragraph, the official or entity shall permanently destroy the location information in accordance with subsection (d).
- d. On expiration of the applicable retention period under this section, the government official or government entity shall permanently destroy the location information and any copies of the information in a manner that renders the information unrecoverable.

Section 7. Enforcement Provisions.

- a. Location information accessed in violation of this Act is not admissible as evidence in any criminal, civil, or administrative proceeding.
- b. If a government entity learns that a government official within that government entity has violated any provision of this Act, the government entity shall suspend that government official's access to any database that contains location information:

1. for seven days upon a first violation;
 2. for 30 days upon a second violation; and
 3. permanently upon a third or subsequent violation.
- c. If the Attorney General has reason to believe that a government official or government entity has violated any provision of this Act, the Attorney General may bring a civil action for declaratory or injunctive relief to prevent any ongoing or future violations.
 - d. Nothing in this section precludes a government official or government entity from taking additional or more severe disciplinary action on learning of a violation of any provision of this Act.

Section 8. Local Regulation.

No municipality or other political subdivision of this state may enact an ordinance, regulation, or policy that allows government officials or government entities to access, retain, or share location information in a manner less restrictive than provided by this Act.