Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Public Safety Committee

HB 1639

Brief Description: Concerning technology-enhanced government surveillance.

Sponsors: Representatives Taylor, Goodman, Morris, Shea, Walkinshaw, Smith, Ryu, Appleton, Condotta, Moscoso, Kagi, Muri, Young, Scott, Schmick, G. Hunt and Farrell.

Brief Summary of Bill

- Prohibits a state agency from procuring an extraordinary sensing device (ESD) unless moneys are appropriated by the Legislature for this express purpose and prohibits a local agency from procuring an ESD without explicit approval of its governing body.
- Requires agencies to publish written policies for the use of ESDs and to minimize collection and disclosure of personal information (PI).
- Prohibits an agency from operating an ESD and disclosing PI unless specifically authorized by the act.
- Allows an agency to operate an ESD if the agency does not intend to collect PI.
- Allows an agency to operate an ESD and disclose PI from the operation if the agency obtains a search warrant, if certain emergencies situations exist, and in specified other circumstances.
- Excludes all evidence collected by an ESD from all court, legislative, or regulatory proceedings if the collection or disclosure of PI violates any provision of this act.
- Creates a legal of action for damages where an individual claims a violation of this act injured his or her business, person, or reputation.
- Requires agencies to maintain records related to each use of an ESD and file an annual report with the Office of Financial Management.

Hearing Date: 2/4/15

Staff: Cassie Jones (786-7303).

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

Background:

Unmanned Aircraft Systems.
An unmanned aircraft system (UAS) is an unmanned aircraft (UA) and all of the associated support equipment necessary to operate the UA. The UA is the flying portion of the system, flown by a pilot via a ground control system, or autonomously through use of an on-board computer, communication links, and any additional equipment. The Federal Aviation Administration (FAA) first authorized the use of UAs in the National Airspace System (NAS) in 1990.

Today, UAs are flying in the NAS under controlled conditions, and are involved in border and port surveillance, scientific research and environmental monitoring, uses by law enforcement agencies, state universities' research, and various other missions for government entities. Operations range from ground level to above 50,000 feet, depending on the specific type of aircraft. Currently, UAS operations are not authorized in Class B airspace, which exists over major urban areas and contains the highest density of manned aircraft in the NAS.

Constitution Limitations.
The Fourth Amendment of the United States Constitution protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Article 1, section 7 of the Washington State Constitution provides, "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." These provisions have been interpreted by courts to prohibit the government or a state actor from conducting certain searches of individuals without a warrant issued by a court of competent jurisdiction. This prohibition is enforced by excluding evidence obtained in violation of the warrant requirement, unless an exception applies. However, many kinds of government surveillance are not considered a search requiring a warrant under the federal or State Constitution. This may include surveillance of activities occurring in open fields or in plain view, and sometimes, the government's acquisition of information from a third-party. Congress and state legislatures may choose to establish stronger regulations on government surveillance than the floor established by either the federal or states constitutions.

Summary of Bill:

General Rule.
It is unlawful for an agency to operate an extraordinary sensing device (ESD) or use or disclose personal information (PI), defined as all information relating to a particular identified or identifiable individual, unless specifically authorized by the act.

Procurement and Policies for Use of ESDs.
State and local agencies must make publicly available written policies for use of ESDs and provide notice and opportunity for comment prior to adoption. No agency may procure an ESD unless money is expressly appropriated by the Legislature for this purpose, or a local agency's governing body has given explicit approval. All agency operations of an ESD and disclosure of PI must be conducted in such a way as to minimize unauthorized collection and disclosure of PI.

Agency Use Not Intended to Collect PI.

An agency may operate an ESD if it reasonably determines that the operation does not intend to collect PI. Agencies may not attempt to identify an individual from the information collected or associate the information with an individual or disclose the information to a third-party unless there is probable cause that the information is evidence of criminal activity.

Agency Use.
An agency may operate an ESD and disclose PI if the agency obtains a search warrant. Search warrants may not be issued for a period greater than 10 days with a possible extension of up to 30 days. A copy of the warrant must be served upon the target within 10 days of its execution. Notice can be delayed if a court finds that it may create an adverse result. An adverse result is: endangering the life or safety of an individual, causing a person to flee from prosecution, destruction of evidence, or intimidation of a witness, or jeopardizing an investigation, or delaying a trial.

Agency Use in Specific Circumstances.
An agency may operate an ESD and disclose PI under the following circumstances:

- an emergency situation exists that involves criminal activity and presents immediate danger of death or serious physical injury to a person, requires operation of an ESD before a warrant can be obtained, and there are grounds upon which a warrant could be granted;
- an emergency situation exists that does not involve criminal activity, presents immediate danger of death or serious physical injury to a person, and operation of an ESD can reasonably reduce the danger;
- a training exercise conducted on a military base and the ESD does not collect PI on persons located outside the base;
- for training, testing, or research purposes not intended to collect PI from individuals without their written consent; or
- in response to a state of emergency proclaimed by the Governor.

Use, Disclosure, and Retention of PI.
Personal Information collected by an agency during operation of an ESD may not be used, copied, or disclosed unless there is probable cause that the PI is evidence of criminal activity. Personal Information must be deleted within 30 days if the PI was collected on a target of a warrant or within 10 days for other PI; this time period runs from the point at which there is no longer probable cause that the PI is evidence of criminal activity. Deletion is only required to the extent that it can be done without destroying other evidence relevant to a criminal case. Personal Information is presumed not to be evidence of criminal activity if the PI is not used in a criminal prosecution within one year of collection.

Exclusionary Rule.
All PI, and any evidence derived from it, is inadmissible in any proceeding before a court, regulatory body, legislative committee, or other authority, if the PI was obtained in violation of any provision in the act.

Private Cause of Action.
Any person who knowingly violates the act is subject to a legal action for damages by any person claiming injury of his or her business, person, or reputation. The injured person is entitled to reasonable attorneys' fees and other costs of litigation.

Records Retention and Reporting.
Agencies having jurisdiction over criminal law or regulatory enforcement must maintain records for each operation of an ESD and must submit a report to the Office of Financial Management (OFM). The records maintained by the agencies must include:

- the number of ESD operations and their justifications;
- the number of criminal and regulatory investigations aided by an ESD and how it was helpful;
- the frequency and type of data collected for individuals other than targets;
- the cost of the ESDs;
- the dates that PI and other data was destroyed;
- the number of warrants requested, issued, and extended; and
- tther information requested by the governing body.

Other agencies must also maintain records for each operation of an ESD and must submit a report to the OFM. The records maintained by the agencies must include:

- the types of ESDs used and the purposes for their use, and the name of the person who authorized the use;
- whether the ESD was imperceptible to the public;
- the kinds of PI collected;
- the length of time the PI was retained;
- steps taken to mitigate the impact on privacy, including the data minimization protocol; and
- an individual point of contact for citizen complaints.

The OFM must compile the results and submit them to the Legislature each year.

Appropriation: None.

Fiscal Note: Requested on January 28, 2015.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.