HOUSE BILL REPORT
ESHB 1639

As Amended by the Senate

Title: An act relating to technology-enhanced government surveillance.

Brief Description: Concerning technology-enhanced government surveillance.

Sponsors: House Committee on Public Safety (originally sponsored by Representatives Taylor, Goodman, Morris, Shea, Walkinshaw, Smith, Ryu, Appleton, Condotta, Moscoso, Kagi, Muri, Young, Scott, Schmick, G. Hunt and Farrell).

Brief History:
Committee Activity:
Public Safety: 2/4/15, 2/13/15 [DPS].
Floor Activity:
Passed House: 3/4/15, 73-25.
Senate Amended.
Passed Senate: 4/15/15, 43-4.

Brief Summary of Engrossed Substitute Bill

- Prohibits state agencies from procuring an extraordinary sensing device (ESD) without an appropriation by the Legislature 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.
- Prohibits agencies from operating an ESD and disclosing personal information unless specifically authorized by the act.
- Allows agencies to operate an ESD without obtaining a warrant if the agency does not intend to collect personal information.
- Allows agencies to operate an ESD and disclose personal information from the operation under certain circumstances.
- Excludes all evidence collected by an ESD from all court, legislative, or regulatory proceedings if the collection or disclosure of personal information violates any provision of this act.

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.

- Creates a legal cause 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.

HOUSE COMMITTEE ON PUBLIC SAFETY

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 6 members: Representatives Goodman, Chair; Orwall, Vice Chair; Hayes, Assistant Ranking Minority Member; Griffey, Moscoso and Wilson.

Minority Report: Do not pass. Signed by 3 members: Representatives Klippert, Ranking Minority Member; Appleton and Pettigrew.

Staff: Cassie Jones (786-7303).

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 Engrossed Substitute 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 Uses Without a Warrant.
An agency may operate an ESD without obtaining a warrant 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.

An agency may operate an ESD and disclose PI without obtaining a warrant under the following circumstances:

- an emergency 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 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.

Agency Uses With a Warrant.
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, jeopardizing an investigation, or delaying a trial.

Use, Disclosure, and Deletion 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
- other 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.

EFFECT OF SENATE AMENDMENT(S):

The Senate amendment:

- removes the definition of "personal information" replaces it with "personally identifiable information";
- defines "personally identifiable information" as any information that can be used to distinguish or trace an individual's identity that includes, but is not limited to, name, Social Security number, and biometric record, either alone, or when combined with other information linked or linkable to a specific individual including, but not limited to, date and place of birth and mother's maiden name;
- replaces all references to "personal information" with "personally identifiable information"; and
- provides that the act expires on July 1, 2020.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

(In support) This is not a partisan issue. Partisan politics end when it comes to protecting freedom and liberty. This bill improves upon last year's bill which passed both chambers. During the interim there was a Governor's task force that did not reach consensus. However, a lot of that work was included in this bill. The bill is streamlined and more readable. The definitions are simplified. The definition of "personal information" is narrowed. Agency authority is clarified. Reporting requirements are streamlined. A clear and reasonable framework for use of ESDs is needed. The scheme focuses on outlawing warrantless surveillance. There are warrantless, allowable uses. This bill contains reasonable compromise. Transparency and accountability measures are included. Regarding public disclosures, deletions of data are appropriate where the data is not being used. This protects individual privacy. There is no reason for anyone to acquire the information collected accidentally. This technology is a game changer and allows for cheap, ubiquitous surveillance. The Legislature is in the best position to create these laws. This should not be left to the courts because uncertainty is bad for all. There is a lack of clarity on drone regulations that negatively affects researchers. Researchers are hesitant to use their talent and time to develop drone applications for agency needs because regulations for drone uses are uncertain. Drones offer many possibilities for beneficial uses. Aerial inspections of land owners should only be done with permission of the land owners. Legislators need to provide the guidance for the use by the government. There is a concern that agencies will fly over farmlands without warrants.

(In support with concerns) This bill needs enhancements. Several sections allow extensive use of information without a warrant in a criminal prosecution. Information collected should always require a warrant prior to use in a criminal court. A warrant, an established exception, or consent should be required before any information collected from a drone is used in court.

(With concerns) Many state agencies believe that the various proposals for the use of drones prevents agency use. The bill changes plain view doctrine and jurisprudence regarding the expectation of privacy in public. There are many potential beneficial uses for UAs, including scientific and enforcement uses. The uses will promote cost savings and efficiencies. Restricting the use of UAs to private locations where there is an expectation of privacy is responsible. There is a lower expectation of privacy on public land. The bill eliminates open fields doctrine where law enforcement is using a UA. In addition, the destruction of data required after one year does not align with the statute of limitations of many crimes.

There is a problem with the definition of PI and issues regarding public disclosure. Many of the items included in PI are not really PI as currently defined in statutes. References to disclosure in the bill should be removed. There should be access to information properly and improperly gathered. There is a private right of action created in the bill, but the bill requires evidence supporting the cause of action to be destroyed. There is a prior restraint provision in the bill that would not stand a court challenge. Fears regarding older technologies once thought to be game-changing have abated.

(Opposed) The definition of PI in the bill is too expansive. It could include a ship that spills oil in the public waters. The definition is vague and would put the agency at-risk due to uncertainty about what is included in the PI definition. There is concern about agencies using data gathered by third parties that are not subject to the bills' restrictions and whether state agencies would be permitted to use this information. Piloted aircraft are being used within the current privacy laws; use of drones would be more efficient and effective.

The state Constitution already protects individuals from privacy invasions, and has protected individuals over time and with each new technology used by police. There is a diminished expectation of privacy in a public place. This applies to all types of technology. There are a lot of conspiracy theories about drones; legislation should not be based on fear. There are no deficiencies in the state Constitution. The court's decisions are based on the behavior and whether it violates another's privacy; it does not presuppose that certain technology is bad, as this bill does.

Persons Testifying: (In support) Representative Taylor, prime sponsor; Shankar Narayan and Doug Klunder, American Civil Liberties Union of Washington; Don Wang; Lee Colleton, Seattle Privacy Coalition; and Tom Davis, Washington Farm Bureau.

(In support with concerns) Kent Underwood, Washington Association of Criminal Defense Lawyers and Washington Defender Association.

(With concerns) Sandy Mullins, Office of the Governor; Joanna Eide, Department of Fish and Wildlife; and Rowland Thompson, Allied Daily Newspapers.

(Opposed) Jessica Archer, Department of Ecology; and James McMahan, Washington Association of Sheriffs and Police Chiefs.

Persons Signed In To Testify But Not Testifying: None.