SENATE BILL REPORT
ESHB 1639

As of March 24, 2015

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: Passed House: 3/04/15, 73-25.
Committee Activity: Law & Justice: 3/17/15.

SENATE COMMITTEE ON LAW & JUSTICE

Staff: Tim Ford (786-7423)

Background: A remotely piloted aircraft, commonly known as a drone, is an aircraft without a human pilot onboard. The flight is controlled either autonomously by computers onboard, or under the remote control of a pilot on the ground or in another vehicle. There are a wide variety of drone shapes, sizes, configurations, and characteristics. There are also a wide variety of applications for drones: military, law enforcement, agriculture, business, recreation, and criminal or nefarious drone enterprises.

In 2012 the Federal Aviation Administration (FAA) established the Unmanned Aircraft Systems (UAS) Integration Office to provide a one-stop portal for certification of civil and public drone operations in national airspace. By the fall of 2015, Congress requires that the FAA integrate remotely piloted aircraft throughout U.S. airspace. The FAA has authorized limited drone operations for important missions in the public interest, such as firefighting, disaster relief, search and rescue, law enforcement, border patrol, military training, and testing and evaluation. In February 2015, the FAA proposed regulations that would allow routine commercial use of small UAS – under 55 pounds. The FAA proposal would limit flights to daylight and visual-line-of-sight operations. It also addresses height restrictions, operator certification, optional use of a visual observer, aircraft registration and marking, and operational limits.

Model aircraft are also unmanned aircraft. FAA guidance says that model aircraft flights should be kept below 400 feet above ground level, should be flown a sufficient distance from

---

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.

populated areas and full scale aircraft, and are used for recreational, rather than business, purposes.

Some states have enacted laws or regulations for drone uses. Washington State law does not regulate drone uses.

Constitution Limitations. The Fourth Amendment of the U.S. 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 from conducting searches of individuals or property without a warrant. This prohibition is enforced by excluding evidence obtained in violation of the warrant requirement, unless an exception applies. However, the courts have reviewed the use of surveillance technology on a case-by-case basis, and some types of surveillance technology do not require a warrant for their use. 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.

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 an 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 for a specified use. 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, 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 ten days with a possible extension of up to 30 days. A copy of the warrant must be served upon the target within ten 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. PI 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. PI must be deleted within 30 days if the PI was collected on a target of a warrant or within ten 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. PI 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 the person's 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 following:

- 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 OFM. The records maintained by the agencies must include the following:

- 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.

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

Appropriation: None.

Fiscal Note: Available.

Committee/Commission/Task Force Created: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony: PRO: Drones are a game-changing technology. They can be used to conduct surveillance without a citizen being aware. People have an expectation of privacy. The bill is improved from last session. It includes a clearer definition of personal information about an individual. It allows warrantless use of drones for emergencies. Data should not be held by agencies after its use has been fulfilled. The plain-view doctrine should not be the same as the old technology of helicopters. The bill creates a clear and reasonable framework for the use of drones and allows agencies to make public their policies for drone uses. It also requires minimization of personal information collected. Personal private information should not used in court unless it complies with the Washington Constitution.

CON: The Governor vetoed a similar bill for reasons such as an overly broad definition of personal information, shifting jurisprudence around the open view doctrine, and a public disclosure provision which had a very short timeframe over what information must be deleted. We still have concerns about this bill's broad definition of personal information and public disclosure. The definition of personal information is so broad that it may prohibit use of drones entirely. The open view doctrine is degraded by the bill. Legislation should address a person's action and not be based on the technology. People don't have an expectation of privacy in a public space. State agencies are not using drones as there is a moratorium until legislation can be promulgated. Drones are potentially very useful tools for many beneficial purposes like wildlife management, air quality monitoring, and other uses. Drones allow agencies to do more work efficiently with less money. Drones are not a game-changing technology and they fit within the framework of the Public Records Act.

Persons Testifying: PRO: Representative Taylor, prime sponsor; Shankar Narayan, American Civil Liberties Union of WA; Lee Colleton, Seattle Privacy Coalition; Patricia Fulton, WA Criminal Defense Lawyers, WA Defenders Assn.

CON: Sandy Mullins, Governor's Office; Jessica Archer, Dept. of Ecology; Joanna Eide, Dept. of Fish and Wildlife; James McMahan, WA Assn. of Sheriffs and Police Chiefs; Rowland Thompson, Allied Daily Newspapers of WA.

Persons Signed in to Testify But Not Testifying: No one.