HOUSE BILL REPORT
EHB 2789

As Passed House:
February 17, 2014

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

Brief Description: Concerning technology-enhanced government surveillance.

Sponsors: Representatives Taylor, Goodman, Shea, Morris, Smith, Walkinshaw, Overstreet, Condotta, Moscoso, Ryu, Short and Scott.

Brief History:
Committee Activity:
None.
Floor Activity:
Passed House: 2/17/14, 83-15.

Brief Summary of Engrossed Bill

- Imposes restrictions on state and local agency procurement and usage of extraordinary sensing devices, defined as unmanned aircraft systems.

Staff: Sarah Koster (786-7303).

Background:

Unmanned Aircraft Systems.
The Federal Aviation Authority (FAA) first authorized the use of unmanned aircraft systems (UAS), in the national airspace in 1990. The FAA defines unmanned aircraft as "a device used or intended to be used for flight in the air that has no onboard pilot."

In 2012 the FAA established the Unmanned Aircraft Systems Integration Office to provide a one-stop portal for civil and public use of UAS in the United States airspace. This office is developing a comprehensive plan to integrate and establish operational and certification requirements for UAS. It will also oversee and coordinate UAS research and development.

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.

There are currently two ways to get FAA approval to operate a UAS. The first is to obtain an experimental airworthiness certificate for private sector (civil) aircraft to do research and development, and training and flight demonstrations. The second is to obtain a Certificate of Waiver or Authorization (COA), which can only be obtained by federal, state, or local governmental agencies.

Constitutional Restrictions.
The federal and state Constitutions prohibit the government or a state actor from conducting certain searches without a warrant issued by a court of competent jurisdiction. This prohibition is enforced by requiring exclusion of 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 often, the government's acquisition of information from a third party. Due to changes in technology, including the increasing deployment and decreasing costs of cameras mounted on unmanned aircraft and satellites, there is growing concern that activities that were formerly private may now be subject to more frequent surveillance, whether such surveillance is conducted by the government or by third parties who acquire personal information about individuals and then make it commercially available to others, including the government.

Congress and state legislatures may establish stronger regulations on government surveillance than the floor established by the Constitution. For example, wiretap laws in Washington regulating the interception of private communications are more restrictive than the requirements established by the Constitution or by federal law, making it a crime under certain circumstances to intercept a private communication without the consent of all parties to the communication.

Summary of Engrossed Bill:

Definitions.
"Agency" means the state of Washington, its agencies, and political subdivisions, including county and city governmental entities, and includes any entity or individual, whether public or private, with which any of the governmental entities has entered into a contractual relationship or any other type of relationship, with or without consideration, for the operation of an extraordinary sensing device that acquires, collects, or indexes personal information to accomplish an agency function.

"Extraordinary Sensing Device" (ESD) means an unmanned aerial vehicle.

"Governing Body" means the council, commission, board, or other controlling body of an agency in which legislative powers are vested, except that for a state agency for which there is no governing body other than the Legislature, governing body means the chief executive officer of the agency.

"Personal information" means all information that:

- describes, locates, or indexes anything about a person including, but not limited to: (1) his or her social security number, driver's license number, agency-issued identification number, student identification number, real or personal property holdings derived from tax returns, and the person's education, financial transactions, medical history, ancestry, religion, political ideology, or criminal or employment record; or (2) intellectual property, trade secrets, proprietary information, or operational information;
- affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such person; and the record of the person's presence, registration, or membership in an organization or activity, or admission to an institution; or
- indexes anything about a person including, but not limited to, his or her activities, behaviors, pursuits, conduct, interests, movements, occupations, or associations.

Procurement.
A state criminal justice agency, including the Washington State Patrol, may not procure an ESD without the explicit approval of the Legislature, given for that device for that specific purpose.

A local law enforcement agency may not procure an ESD without the explicit approval of the local governing body, given for that device, for that specific purpose.

A state or local agency seeking to use an ESD for one of the following enumerated purposes must first obtain explicit approval of the agency's governing body:
- Monitoring to discover, locate, observe, or prevent forest fires.
- Monitoring an environmental or weather-related catastrophe or damage from such an event.
- Surveying for wildlife management, habitat preservation or environmental damage.
- Surveying for assessment & evaluation of environmental or weather-related damage, erosion, flood or contamination.
- Training and testing which does not collect personal information outside a military base.
- Responding to an emergency, for which the Governor has proclaimed a state of emergency.

Usage.
No agency, including the state, its agencies, and any political subdivisions, such as county and city governmental entities, may use an ESD except as specifically authorized by the bill.

An agency may only use an ESD pursuant to a judicially issued search warrant or under one of the following exceptions:
- for a non-criminal emergency with immediate danger of death of serious bodily injury, if the ESD is required;
- for a criminal emergency, with immediate danger of death or serious bodily injury and no time to obtain a warrant. In this case, a warrant must be obtained after the fact;
- for training or testing if no personal information is collected outside a military base;
- for emergency response if there is a Governor-declared state of emergency; or

- for an operation unlikely to collect personal information and not for regulatory enforcement, limited to the following:
    - Monitoring to discover, locate, observe, or prevent forest fires
    - Monitoring an environmental or weather-related catastrophe or damage from such an event.
    - Surveying for wildlife management, habitat preservation or environmental damage.
    - Surveying for assessment & evaluation of environmental or weather-related damage, erosion, flood or contamination.

No regulatory usage is allowed until the Legislature has specifically permitted it via legislation.

To obtain a search warrant, an agency must assert that other methods of data collection are unacceptable because of cost or danger. A warrant may be issued for up to 10 days, or extended up to 30 days, if deemed necessary by a judicial officer. A copy of the warrant must be served on the target within 10 days, unless there is a reason to believe a specifically enumerated adverse result, such as destruction of evidence or intimidation of witnesses, would occur, unless a judicial extension is granted.

Any agency using an ESD must develop written policies and procedures for ESD use and make those policies and procedures public.

An ESD operated by an agency must have a unique identifier registration number affixed to it and the number must be designed to be viewable by the public, as far as practicable, while the ESD is in use.

Information management.
No agency may disclose personal information acquired through operation of an ESD except as specifically authorized by the bill. All operations of ESD and disclosure of personal information must be done to minimize the personal information impacted.

Personal information collected by ESDs may not be used, copied, or disclosed except if there is probable cause that the information is evidence of criminal activity. There must be a determination within 10 days (or 30 days if the information is about the subject of the warrant) if the information is evidence of criminal activity and, if not, the information must be deleted within that same time period.

Personal information may not be received in evidence if it was collected or disclosed in violation of the bill.

Recordkeeping and Reporting.
All state agencies which use ESDs must maintain records of each use of an ESD and, for each year in which an ESD was used, prepare an annual report. Each report shall include, at a minimum, the types of ESDs used, the circumstances of use, the collection, management and deletion of personal information, and the use of the data. The reports will be compiled by the Office of Financial Management and submitted electronically to the Legislature by September 1 of each year.

All local law enforcement agencies using ESDs must maintain records of each use including, at a minimum, the number and types of uses, the frequency, type and deletion schedule of collected personal information, and the use of data collected for investigations.

Penalties.
Anyone who claims that a violation of the bill's provisions has injured his or her business, person, or reputation may sue for actual damages or liquidated damages of $1 per day per violation, as well as attorney's fees, and other costs of litigation.

Appropriation: None.

Fiscal Note: Not requested.

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