

HOUSE BILL REPORT

HB 2789

As of Second Reading

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 and Condotta.

Brief History:

Committee Activity:

None.

Brief Summary of 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.

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

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.

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 Bill:

Washington agencies and political subdivisions, including county and city governments, may only procure or operate an extraordinary sensing device (ESD) or use or disclose personal information acquired through ESD, under the circumstances specified in the bill.

Definitions.

An ESD is defined in the bill to refer only to an unmanned aircraft system.

"Personal information" means all information that: (1) describes, locates, or indexes anything about a person including, but not limited to, the person's 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; (2) 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 (3) describes, locates, or indexes anything about a person including, but not limited to, intellectual property, trade secrets, proprietary information, or operational information.

"Agency" means the state of Washington, its agencies, and political subdivisions and includes any entity, whether public or private, with which any of the governmental entities has entered into a contractual relationship for the operation of a system of personal information or unmanned aircraft system to accomplish an agency function.

Procurement.

An agency, state or local, must obtain explicit approval from the agency's governing body (which may be the agency's chief executive officer) before procuring an ESD.

Usage.

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 or 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
- For an operation unlikely to collect personal information and not for regulatory enforcement, including, but not limited to, environmental or wildlife monitoring or assessment.

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.

Information Management.

All operations of ESD and disclosure of personal information must be done to minimize the personal information impacted.

Personal information collected by ESD 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.

Reporting.

Any agency which procured or used an ESD in a year must prepare an annual report, publically available electronically, which describes the types of ESD used, the purpose and circumstances of use, the steps taken to mitigate impacts on privacy, and a point of contact for citizen complaints. the report must be made to the agency governing body or the Office of Financial Management.

Penalties.

Anyone who claims that a violation of the bill's provisions has injured his or her business, person, or reputation may sue for damages, attorney's fees, and other costs of litigation.

Codification.

The bill creates a new subchapter of Chapter 9.73 RCW.

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.

Staff Summary of Public Testimony:

(In support) None.

(Opposed) None.

Persons Testifying: None.

Persons Signed In To Testify But Not Testifying: None.