SENATE BILL REPORT
EHB 2789

As Reported by Senate Committee On:
Law & Justice, February 28, 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: Passed House: 2/17/14, 83-15.
Committee Activity: Law & Justice: 2/26/14, 2/28/14 [DPA].

SENATE COMMITTEE ON LAW & JUSTICE

Majority Report: Do pass as amended.
Signed by Senators Padden, Chair; O'Ban, Vice Chair; Kline, Ranking Member; Darneille, Pearson, Pedersen and Roach.

Staff: Tim Ford (786-7423)

Background: An unmanned aircraft system (UAS), 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 UAS shapes, sizes, configurations, and characteristics. There are also a wide variety of applications for drones: military, law enforcement, agriculture, business, etc.

In 2012 the Federal Aviation Administration (FAA) established the Unmanned Aircraft Systems Integration Office to provide a one-stop portal for certification of civil and public UAS 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 UAS 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. 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 populated areas and full scale aircraft, and are used for recreational, rather than business, purposes.

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.

Thirteen states have enacted laws related to UAS operations by state or local government agencies.

Summary of Bill (Recommended Amendments): Intent. It is the intent of the Legislature to provide clear standards for the lawful use of unmanned aerial vehicles by state and local jurisdictions.

Definitions. Unmanned aircraft means an aircraft that is operated without the possibility of human intervention from within or on the aircraft.

Extraordinary sensing device (ESD) means a sensing device attached to an unmanned aircraft. Sensing device means a device capable of remotely acquiring personal information using any frequency of the electromagnetic spectrum, or a sound-detecting system.

Agency means the state of Washington and its agencies and subdivisions, including entities contracting with agencies to operate an ESD, but excludes the Washington National Guard. Governing body means the controlling legislative body of an agency, except that of a state agency for which there is no governing body other than the state Legislature. Governing body means the chief executive officer for the agency.

ESD Operations. It is unlawful to operate an ESD except as provided. For criminal law and regulatory law enforcement ESD operations, a state agency must obtain approval from the Legislature and a local agency must obtain approval from its governing body. Approvals must be explicit and specific to an ESD and a particular purpose.

Authorized ESD operations by a public agency must be conducted to minimize the collection and disclosure of personal information. All ESDs must comply with FAA requirements. Nothing in this chapter is construed to limit the state's ability to establish and operate a test range for the integration of unmanned aviation vehicles into the national airspace. ESD operations are prohibited unless an agency affixes an identification registration number.

An ESD may be operated pursuant to a criminal search warrant where law enforcement demonstrates in writing probable cause of a criminal violation. A warrant may not exclude the collection of biometric data. Warrants are limited to 10 days and an extension may be granted for no longer than 30 days. Within 10 days, law enforcement must serve a copy of the warrant on the person whose personal information was collected. A court may allow the delayed service of a warrant for no longer than 90 days where service may cause an adverse result such as endangering the safety of a person or jeopardizing an investigation.

Warrant Exceptions. A law enforcement officer or public official may use an ESD and disclose personal information gathered without a warrant if the officer reasonably determines that an emergency situation exists which presents immediate danger of death or serious physical injury to any person.

For an emergency that involves criminal activity:

- the emergency must require operation of an ESD before a judicial warrant could be obtained;

- there must be grounds to support a warrant; and
- an application for a warrant must be made within 48 hours of beginning the operation.

When a warrant application is denied, personal information obtained is in violation of the act; however, such violations may not be the basis for legal liability.

If the emergency does not involve criminal activity:

- the emergency has characteristics such that the operation of an ESD can reasonably reduce the danger of death or serious physical injury;
- the operation is for limited environmental operations where it is not intended to and is unlikely to collect personal information, and the operation is not for purposes of regulatory enforcement;
- the operation is training on a military base;
- the operation is for training, testing, or researchby an agency and does not collect personal information without written consent; or
- the operation is in response to a gubernatorial proclamation of an emergency or disaster.

Upon completion of the warrantless ESD operation all personal information collected must be destroyed within 24 hours.

Use of Personal Information Prohibited. Information collected in violation of this law or evidence derived thereof is inadmissible in a court, agency, regulatory body, or other authority. Personal information collected in compliance with this law may not be used, copied, or disclosed after the conclusion of the operation unless there is probable cause that the information is evidence of criminal activity. Personal information must be deleted where there is no longer probable cause within 30 days if the information was collected on the target of the warrant, and within ten days if the information was collected incidentally to the operation. A presumption exists that personal information is not evidence of criminal activity if not used in a criminal prosecution within one year.

Liability for Damages. Any person is legally liable for damages caused by knowing violations of this act. Damages are limited to actual damages, and also reasonable attorney fees and other litigation costs.

Recordkeeping and Reporting. Each agency must publish policies for ESD uses, including on the agency website, and provide notice and opportunity for public comment prior to adoption. Agencies must maintain records of each ESD use. Annual detailed reports by agencies related to all ESD uses must be provided to the Office of Financial Management which compiles the results for legislative committees. The reports must include detailed descriptions of the kind of warrants requested, details about the warrants and the information gathered, the number of resulting arrests, and the cost of the resources used in the operations.

EFFECT OF CHANGES MADE BY LAW & JUSTICE COMMITTEE (Recommended Amendments): The definitions of a biometric identification system is removed. ESD means a sensing device attached to an unmanned system, not the UAS itself and includes sound-sensing devices. Agency excludes the Washington National Guard.

Allows agencies with criminal and regulatory enforcement jurisdiction to obtain authority to procure drones.

The restriction on the use of a biometric identification system pursuant to a warrant is removed.

It is lawful for law enforcement or an agency to operate an ESD and disclose personal information if it is reasonably determined that an emergency situation exists that has characteristics such that it would reduce the danger of death or serious injury or the operation is for training or research purposes that does not collect personal information without written consent.

No legislation is required before a drone may be used for investigation or regulatory enforcement.

An identifier registration number is required but does not need to be viewable by the public while the device is in use.

The law is not to be construed to limit the state's ability to establish and operate a test range for integration of drones into national airspace.

Publication of policies must be posted on the agency website.

Damages are limited to actual damages, not liquidated damages.

Appropriation: None.

Fiscal Note: Not requested.

Committee/Commission/Task Force Created: No.

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

Staff Summary of Public Testimony on Engrossed House Bill: PRO: This is a bipartisan bill. It improves on prior versions by providing better procurement, use, and reporting requirements for drones. There is still a question of whether incidental collection of data may be used for criminal purposes and an amendment is in the works. Procurement is not for regulatory enforcement; we will look at that later. The requirement for a drone to be labeled with an identification number is more for liability purposes should it crash. The bill is a reasonable restriction on agency uses of drones so that privacy of citizens will not be compromised. Drones are a useful tool yet they will be pervasive and must be regulated. The FAA does not regulate privacy and states should regulate drone uses by agencies.

CON: The warrant standard is not consistent with current practices. The definition for a drone needs to be more transparent; it is called an ESD and it should just be called what it really is, a UAS. The term independently elected official should be added to section 4(4). Liquidated damages does not make sense because if a drone inadvertently records personal information while flying over Seattle, how does one calculate liquidated damages, one dollar

per person? For more than a century people have had a reasonable expectation of privilege. Drones freak people out but there is no need for the bill. The provisions do not work. The restriction on collecting biometric data renders drones useless for law enforcement purposes. The plain views doctrine is not preserved. The bill needs more work.

OTHER: This meets most of the needs of the Department of Natural Resources but we are waiting to see the amendments. The definition of an ESD is imprecise, not all UASs have sensing devices. The FAA has a better definition for a drone. It is unclear what legal uses are allowed for criminal and regulatory enforcement. The Department of Fish and Wildlife (DFW) enforces many different laws for hydraulic violations, commercial fishing, and coastal shellfish. Commercial fishing is worth hundreds of millions of dollars and drones will be a useful tool to monitor commercial fishing. Our jurisdiction extends out over the water for 200 miles from the coast. We use manned aircraft and find violations, sometimes in remote areas. We do not have plans to purchase drones at this time. The Department of Ecology (Ecology) views the bill as too restrictive and freezing the use of technology. The bill impacts future uses and capabilities to evolve. Personal information may be captured of willing volunteers by the University of Washington (UW) for testing purposes and the bill does not allow it. We need to continue a discussion with agencies and inventory the potential uses of drones by public agencies. A work session is recommended.

Persons Testifying: PRO: Representative Taylor, prime sponsor; Representative Morris; Shankar Narayan, American Civil Liberties Union; Kasey Burton, UW Law School; Mary Verner, Dept. of Natural Resources; Amanda Lee; WA Assn. of Criminal Defense Lawyers.

CON: Don Pierce, WA Sheriffs and Police Chiefs; Rob Huss, WA State Patrol; James McMahan, WA Assn. of County Officials.

OTHER: Nancy Bickford, WA Military Dept.; Jessica Archer, Ecology; Steve Crown, Mike Cenci, DFW Police; Margaret Sheperd, UW; Denny Eliason, Amazon.