

SENATE BILL REPORT

SB 6172

As Reported by Senate Committee On:
Law & Justice, February 6, 2014

Title: An act relating to protecting Washington citizens from warrantless surveillance, reducing liability, and establishing clear standards under which agencies may utilize unmanned aerial vehicles.

Brief Description: Protecting Washington citizens from warrantless surveillance, reducing liability, and establishing clear standards under which agencies may utilize unmanned aerial vehicles.

Sponsors: Senators Hargrove, Chase, Rivers, Rolfes, Benton, Hasegawa, Baumgartner, Kohl-Welles, Litzow, Darneille, Keiser, Pedersen and Kline.

Brief History:

Committee Activity: Law & Justice: 1/27/14, 2/06/14 [DPS].

SENATE COMMITTEE ON LAW & JUSTICE

Majority Report: That Substitute Senate Bill No. 6172 be substituted therefor, and the substitute bill do pass.

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 an unmanned aerial vehicle or 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.

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

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.

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

Summary of Bill: The bill as referred to committee not considered.

Summary of Bill (Recommended Substitute): 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.

Public unmanned aircraft system (PUAS) means an unmanned aircraft and associated elements, including communications links, sensing devices, and the components that control the unmanned aircraft, operated by, at the direction of, or under the control of an agency.

Agency means all state governmental entities, except the Washington National Guard, or any local government, and also any entity which contracts with an agency to operate a UAS.

PUAS Operations. It is unlawful to operate a PUAS except as provided. For PUAS operations, a state agency must obtain approval from the Legislature and a local agency must obtain approval from the local governing body of the local agency. The approval must be explicit and specific to a PUAS and a particular purpose. All PUAS operations must be conducted to minimize collection and disclosure of personal information. All UASs must comply with FAA requirements. The state may establish a test range for the integration of unmanned aerial vehicles into national airspace.

A PUAS may be operated pursuant to a criminal search warrant where law enforcement demonstrates in writing probable cause of a criminal violation. Warrants are limited to ten days and an extension may be granted for no longer than 30 days. Within ten 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 a PUAS and disclose personal information gathered by a PUAS 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.

If the emergency involves criminal activity:

- the emergency must require operation of a PUAS 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.

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

If the emergency does not involve criminal activity:

- the emergency must require operation of a PUAS to reduce the danger of death or serious physical injury;
- the operation does not intend 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 and testing by an agency and does not collect personal information; or
- the operation is in response to a gubernatorial proclamation of an emergency or disaster.

Upon completion of the warrantless PUAS 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 10 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.

Reporting Requirements. Annual reports of the PUAS warrants requested and granted are required as follows:

- judicial officers who issue warrants for a PUAS must report to the Chief Justice of the Supreme Court;
- agencies which used a PUAS without warrants must report to the Chief of the Washington State Patrol; and
- the Chief Justice and the Chief of the Washington State Patrol must provide a report, including a summary analysis of all reported data, to the Legislature.

The reports must include 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.

Additional Requirements for Localities. Governing bodies for localities must do the following:

- publish written policies and procedures for PUAS operations by law enforcement;
- require, by ordinance, law enforcement to maintain records of each use of a PUAS; and
- conduct annual audits of all PUAS operations and make the audits publicly available.

The Department of Natural Resources (DNR) may operate PUASs for firefighting and fire prevention without requiring a warrant. DNR drone operations may not be used for law enforcement or regulatory enforcement purposes. Personal information obtained must be destroyed within 30 days after an operation is concluded.

Nothing in this chapter is to be construed either to limit nor expand the case law "plain view" doctrine regarding warrantless search and seizure of evidence by law enforcement.

EFFECT OF CHANGES MADE BY LAW & JUSTICE COMMITTEE (Recommended Substitute as Passed Committee): DNR may operate PUASs for firefighting and fire prevention without requiring a warrant. DNR drone operations may not be used for law enforcement or regulatory enforcement purposes. Personal information obtained must be destroyed within 30 days after an operation is concluded.

Nothing in this chapter is to be construed either to limit nor expand the case law "plain view" doctrine regarding warrantless search and seizure of evidence by law enforcement.

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 on Proposed Substitute as Heard in Committee:
PRO: New and evolving technology is becoming affordable and pervasive. Thirteen states restrict drone uses. In Washington some local jurisdictions have passed restrictions. This legislation is a reasonable limitation and balances the need for surveillance with privacy interests. The new section 12 in the proposed substitute should go back to the language in the original bill since actual damages are hard to quantify. Public uses include search and rescue for lost hikers. Some sections may allow DNR to use drones without an amendment. Farmers are not impacted. This legislation establishes a floor and local governments are not preempted if they want to provide greater protections to privacy. The probable cause standard needs work and the federal wiretap law could be used as a model. This legislation should be submitted for an advisory vote of the people.

CON: Section 11 of the original bill prohibits use of personal information if collected about a non-target. That is unacceptable and it is not clear in the proposed substitute whether information of a non-target may be used. Drone use is already legal and we would be opposed to any erosion of the plain view doctrine. Courts limit some new technology such as infrared vision, if intrusive into privacy, without a warrant. Law enforcement cannot invade privacy without a warrant. Reporting requirements increase Washington State Patrol's workload and agencies operating drones can report directly to the Legislature.

OTHER: DNR would like an amendment expressly authorizing DNR to use drones for firefighting and fire prevention. Section 9 of the substitute bill does not clearly allow such use.

Persons Testifying: PRO: Shankar Narayan, American Civil Liberties Union; William Covington, Kasey Burton, Jacob McCoy, University of WA Law School; Amanda Lee, WA Defenders Assn.; Tamra Smilanich, David Anderson, citizens.

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

OTHER: Mary Verner, John Kaikkonen, DNR.