HOUSE BILL REPORT
HB 2179

As Reported by House Committee On:
Technology & Economic Development
Appropriations Subcommittee on General Government & Information Technology

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

Brief Description: Regarding government surveillance conducted with extraordinary sensing devices.

Sponsors: Representatives Morris and Morrell.

Brief History:
Committee Activity:
Technology & Economic Development: 1/16/14, 1/31/14 [DPS];
Appropriations Subcommittee on General Government & Information Technology: 2/6/14 [DPS(TED)].

Brief Summary of Substitute Bill

- Prohibits Washington, its agencies, and political subdivisions from using an "extraordinary sensing device" (ESD) to conduct surveillance from an "extraordinary vantage point" without a warrant issued by a court of competent jurisdiction, unless an exception applies.
- Provides exceptions from the warrant requirement for certain exigent circumstances, for monitoring for forest fire prevention, for certain environmental or weather-related monitoring and surveying, and for certain surveillance conducted on a military base.
- Enforces violations by excluding unlawfully-obtained personal information from being introduced as evidence in a civil or criminal case.
- Requires agencies to obtain approval from their governing body and follow certain public procedures before procuring an ESD, and to publish annual reports detailing the use and procurement of ESDs.
- Establishes that, in addition to the other requirements concerning government surveillance, an agency may only use an ESD for regulatory surveillance of a permitted or licensed activity if the agency has given clear and conspicuous notice to the permittee or licensee that the activity may be subject to such surveillance.

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.

- Establishes civil liability for intentional violations in the form of damages or liquidated damages, attorneys' fees, and costs.

HOUSE COMMITTEE ON TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 9 members: Representatives Morris, Chair; Smith, Ranking Minority Member; Fey, Freeman, Hudgins, Morrell, Stonier, Tarleton and Wylie.

Minority Report: Do not pass. Signed by 8 members: Representatives Short, Assistant Ranking Minority Member; DeBolt, Kochmar, Magendanz, Ryu, Vick, Walsh and Zeiger.

Staff: Jasmine Vasavada (786-7301).

Background:

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 Substitute Bill:

It is unlawful for Washington agencies and political subdivisions to conduct surveillance with an extraordinary sensing device (ESD) from an extraordinary vantage point, except under circumstances specified in the bill. "Agency" means the state of Washington, its agencies, and political subdivisions, as well as any entity, whether public or private, with which any of the foregoing has entered into a contractual relationship for the operation of a system of

personal information to accomplish an agency function. "Sensing device" means a device capable of remotely acquiring personal information from its surroundings, using any frequency of the electromagnetic spectrum. "Sensing device" does not include equipment whose sole function is to provide information directly necessary for safe air navigation or operation of a vehicle. An "extraordinary sensing device" means a sensing device that: (1) is uncommon to society, meaning that as of January 1, 2014, the sensing device was not generally commercially available to individual consumers at retail stores physically located in the state; and (2) is used in such a manner that it allows personal information to be acquired from an extraordinary vantage point that would not have been easily acquired from an ordinary vantage point. "Extraordinary vantage point" means a vantage point to which an ordinary member of the public does not have ready access.

"Personal information" is broadly defined. It means all information that: (1) describes, locates, or indexes anything about a person including, but not limited to, 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; (2) affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such a 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.

Exceptions.
Washington agencies and political subdivisions may conduct surveillance using an ESD from an extraordinary vantage point if: (1) a court has issued a warrant upon a finding of probable cause; (2) the operation is part of a training exercise conducted on a military base and no personal information is collected on persons located outside the military base; or (3) an emergency situation exists and an application for a warrant is made within 48 hours.

The first exigent circumstance exception is when an agency elected official, appointed official, director, or deputy director reasonably determines that an emergency situation involving criminal activity presents immediate danger of death or serious physical injury to any person and addressing the danger requires operation of the ESD before a warrant authorizing the operation can, with due diligence, be obtained.

The second exigent circumstance exception applies when an agency employee or authorized agent reasonably determines that an emergency situation exists presenting an immediate danger of death or serious physical injury to any person, the purpose of the operation is not investigation of criminal activity and the operation is not intended to collect personal information, and addressing the emergency situation requires operation of an ESD to reduce the danger of death or serious physical injury.

In both cases, an application must be sought within 48 hours after the operation has occurred or begins to occur, surveillance must be immediately terminated when personal information sought is obtained or the warrant application is denied, and any personal information incidentally collected must be deleted within 72 hours of the operation's completion.

In addition, a number of activities are excluded from the definition of "conducting surveillance," as long as the operation is not intended to collect personal information and the purpose is not investigation or criminal activity or regulatory violations or noncompliance:

- monitoring to discover, locate, observe, and 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; and
- surveying for the assessment and evaluation of environmental or weather-related damage, erosion, flood, or contamination.

Government Procurement of Extraordinary Sensing Devices for Surveillance Purposes.
Agencies must obtain approval from their "governing body" before procuring an ESD for surveillance purposes. For state agencies for which there is no commission or body other than the Legislature in which legislative powers are vested, the "governing body" is the chief executive officer responsible for the agency's governance. The governing body shall develop and make available written policies and procedures, and provide notice and opportunity for public comment. Agencies that conduct surveillance using an ESD or procure an ESD must prepare an annual report, stating the types of devices used, the specific kinds of personal information collected, and steps taken to mitigate the impacts on personal privacy, including data minimization protocols, among other categories of information. State agencies shall submit the annual reports to the Joint Legislative Audit and Review Committee (JLARC), who shall compile the results and submit them to the Legislature annually, beginning September 1, 2015.

Exclusionary Rule.
Personal information obtained in violation of these requirements is inadmissible in a civil or criminal case, except:

- in an action for damages brought by a person claiming their rights were violated as a result of a violation of the act's requirements; and
- in a criminal action in which the defendant is charged with a crime, the commission of which would jeopardize national security.

Regulatory Surveillance.
Agencies and political subdivisions are prohibited from using an ESD to conduct surveillance for the purpose of regulatory enforcement, unless:

- the permittee or licensee is given clear and conspicuous notice at the time the permit or license is granted; and
- the agency complies with all of the bill's other requirements for government surveillance.

Civil Liability.
A person who intentionally violates the surveillance restrictions is subject to legal action for damages. Damages may be actual damages or liquidated damages of $1,000 per day, not to exceed $10,000, plus attorneys' fees and costs.

Role of Attorney General.

The Attorney General is encouraged to compile and make available to agencies a list of devices that it has determined to be ESDs. The Legislature states its intent that the Attorney General's determination, made pursuant to the definition of ESDs and stated intent of the bill, be accorded the utmost deference.

Substitute Bill Compared to Original Bill:

The substitute bill makes the following changes compared to the original bill:

- provides that it is generally unlawful for the state of Washington, its agencies, and political subdivisions to conduct surveillance with ESDs from an extraordinary vantage point, without limiting this prohibition to surveillance of private lands;
- provides that the requirement that an agency give clear and conspicuous notice to a permittee or licensee before conducting surveillance for the purpose of regulatory enforcement of a permitted or licensed activity is additional to, and does not replace, the other requirements for government surveillance established in the bill;
- broadens the definition of "agency" to include any entity, whether public or private, with which the state of Washington, its agencies, or political subdivisions has entered into a contractual relationship for the operation of a system of personal information to accomplish an agency function;
- changes the definition of "extraordinary sensing device" to provide that it means a sensing device that: (1) as of January 1, 2014, was not generally commercially available to individual consumers at retail stores physically located in the state; and (2) is used in such a manner that it allows personal information to be acquired from an extraordinary vantage point that would not have been easily acquired from an ordinary vantage point;
- removes from the definition of "conducting surveillance" four activities, as long as the operation is not intended to collect personal information and the purpose is not investigation or criminal activity or regulatory violations or noncompliance. These activities are: (1) monitoring to discover, locate, observe, and prevent forest fires; (2) monitoring an environmental or weather-related catastrophe or damage from such an event; (3) surveying for wildlife management, habitat preservation, or environmental damage; and (4) surveying for the assessment and evaluation of environmental or weather-related damage, erosion, flood, or contamination;
- establishes that the "governing body" who may authorize procurement of an ESD, for state agencies for which there is no commission or body other than the Legislature in which legislative powers are vested, is the chief executive officer responsible for the agency's governance;
- requires agencies, instead of their governing bodies, to prepare annual reports on use and procurement of ESDs;
- requires state agency reports to be compiled by the JLARC, instead of the Washington State Patrol (WSP);
- restricts civil liability for violation of its provisions to violations that are intentional; and
- adds the provision encouraging the Attorney General to compile a list of ESDs and stating the intent that the Attorney General's determination be afforded the utmost deference.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

(In support) Over the interim, the Technology and Economic Development Committee (Committee) looked at issues related to invasive technologies. There are some principles this bill reflects. In the case law, there seems to be some consideration of whether surveillance is covert or can be perceived by ordinary human senses when courts determine whether an expectation of privacy has been violated. If a person is reading a book in the middle of Department of Natural Resources land, the person might have an expectation that no one can see the book that is being read. Another principle this bill is intended to put into action is that technology is neither good nor evil. It is not the delivery method that should matter for regulatory purposes, but what is ultimately done with the technology—the use. The bill does not prohibit government from procuring certain kinds of technologies, but it requires that if a city council is going to make a decision to procure something not readily available to the public, the council needs to make determinations up front instead of on the back end, after the technology has been abused. Years back, when agencies were getting in trouble for dumping personal information out back without shredding it, the Committee did an investigation and learned that a lot of that sensitive personal information need not have been collected to begin with. There is a balance between allowing a technology to be developed and putting on some guard rails, like members of this Committee did with remote frequency identification devices when the Committee established rules of the road, in a manner that allowed those who wished to use the technology to be successful operating it.

This is a conscientious effort to protect privacy for the consumers and residents of this state. There is a two-fold problem. At the local and federal level, surveillance is driven by government demand. Government can hire private companies, both large and small, to conduct surveillance activities. The City of Seattle recently created an initiative to promote Big Data as a business. This aggregates and culls random metadata information and sells it, through data brokerages. Most of these data initiatives result from government demand. This bill should pass out of the Committee so constituents throughout the state, and particularly in western Washington, can weigh in. The remote sensing devices are unfair to the American taxpaying public, who must pay the government to arbitrarily surveil us, without judicial due process. Someone must represent the people's interests in this.

(Opposed) This bill combines a number of new concepts. When a number of broad definitions in the bill are linked together, it makes a very broad statement that is very difficult to understand. A number of legal advisors to the police have reported that they do not know what it all means. But it is clear that a final determination will have to go to a court for interpretation. The definition of an "extraordinary sensing device" will be subject to many interpretations in many courts and many evidentiary hearings will be required. It will give defense attorneys another point to argue about whether evidence should be suppressed. The bill also seems to freeze technology at 2014. That means the WSP would not be able to use

the next version of Google Earth for any criminal investigation in the future, because it will be developed after the 2014 cutoff date and it fits in the definition of "personal information." It seems like ultimately this bill prohibits government from using everything to collect anything. The courts have long dealt with emerging technology. In cases involving global positioning system tracking devices and infrared sensing devices, the courts have applied long-standing principles concerning search and seizure, and those are the rules of the road you are after. The bill should simply require all new technologies to be used in conformance with current laws concerning search and seizure. That may be stating the obvious, but at least you would not need to wait for courts to rule.

The challenge with this legislation is that it attempts to regulate the technology. Both the federal and state constitutions have hundreds of years of experience in protecting people's privacy. The change from horses to cars changed the nature of law enforcement. We did not change our statutes for when parabolic microphones or binoculars were developed. The courts have been really good at striking those continual balances. If somebody invades my privacy, it does not matter how it happened, it matters *that* it happened. That is the principle for the Constitution. The references to activities within the boundaries of somebody's property are troubling. If a law enforcement officer sees a person burying a body in their front yard, they would be allowed to see it with their own eyes, but not with a remote control car. It's not the technology that is the issue, but privacy and the concepts of open space and plain view. The ESD term is very broad. There are significant liabilities for violation of this act. An agency may unintentionally violate this act and suffer a serious penalty. The WSP is required to gather other agency's reports, creating a burden on the WSP without including a compliance requirement. The provisions placing the WSP in this role should be stricken.

Persons Testifying: (In support) Representative Morris, prime sponsor; and Sheila Dean.

(Opposed) Don Pearce and Rob Huss, Washington State Patrol; and James McMahan, Washington Association of County Officials.

Persons Signed In To Testify But Not Testifying: None.

HOUSE COMMITTEE ON APPROPRIATIONS SUBCOMMITTEE ON GENERAL GOVERNMENT & INFORMATION TECHNOLOGY

Majority Report: The substitute bill by Committee on Technology & Economic Development be substituted therefor and the substitute bill do pass. Signed by 5 members: Representatives Hudgins, Chair; Dunshee, S. Hunt, Jinkins and Springer.

Minority Report: Do not pass. Signed by 4 members: Representatives Parker, Ranking Minority Member; Buys, Christian and Taylor.

Staff: Charlie Gavigan (786-7340).

Summary of Recommendation of Committee On Appropriations Subcommittee on General Government & Information Technology Compared to Recommendation of Committee On Technology & Economic Development:

No new changes were recommended.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

(In support) The fiscal note doesn't apply to the new version; some of the technologies noted in the fiscal note, such as night-vision goggles, are not limited by the bill. The bill takes a neutral approach. Technology is not good or evil, it's how the technology is deployed that can cause privacy issues. There are significant issues related to technology and privacy that this bill tries to address. There is a difference between what is obvious surveillance and what is invisible surveillance.

(Opposed) The bill could have significant impact on the Department of Ecology's (DOE) ability to monitor and protect the environment. The DOE uses a variety of technologies, such as infrared and satellite technology, to help inform regulatory decisions and conduct science and research. The DOE looks forward to working with the prime sponsor to balance personal privacy with technologies used to study and protect the environment. This bill is not necessarily about drones, it applies to a variety of technologies like Light Detection and Radar (LIDAR) and electromagnetic spectrums.

Historically, there have been expectations of privacy in one's private affairs compared to the plain view doctrine (no privacy expectation). The bill is well-intentioned but rewrites decades of law related to expectations of privacy. Just because the technology is available to do something doesn't make it okay to do it. This bill would limit law enforcement's ability to do their job. We shouldn't codify standards on a specific date when these standards are modified by the courts over time.

Persons Testifying: (In support) Representative Morris, prime sponsor.

(Opposed) Jessica Archer, Washington Department of Ecology; and James McMahan, Washington Association of County Officials.

Persons Signed In To Testify But Not Testifying: None.