AN ACT Relating to technology-enhanced government surveillance; adding new sections creating a new section; and prescribing penalties.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF

NEW SECTION. **Sec. 1.** The legislature finds that technological advances have provided new, unique equipment that may be utilized for surveillance purposes. These technological advances often outpace statutory protections and can lead to inconsistent or contradictory interpretations between jurisdictions. The legislature finds that regardless of application or size, the use of these extraordinary surveillance technologies, without public debate or clear legal authority, creates uncertainty for citizens and agencies throughout state. The legislature finds that extraordinary surveillance technologies do present a substantial privacy risk potentially contrary to the strong privacy protections enshrined in Article I, section 7 of the state Constitution that reads "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." The legislature further finds that the lack of clear statutory authority for the use of extraordinary

surveillance technologies may increase liability to state and local jurisdictions. It is the intent of the legislature to provide clear standards for the lawful use of extraordinary surveillance technologies by state and local jurisdictions.

NEW SECTION. **Sec. 2.** The definitions in this section apply throughout this section and sections 3 through 13 of this act unless the context clearly requires otherwise.

(1)(a) "Agency" means the state of , its agencies, and political subdivisions.

(b) "Agency" also includes any entity, whether public or private, with which any of the entities identified in (a) of this subsection has entered into a contractual relationship for the operation of a system of personal information or unmanned aircraft system to accomplish an agency function.

(2) "Biometric identification system" is a system that collects unique physical and behavioral characteristics including, but not limited to, biographical data, facial photographs, fingerprints, and iris scans to identify individuals.

(3) "Court of competent jurisdiction" means any district court of the United States or any United States court of appeals that has jurisdiction over the offense being investigated or is located in a district in which surveillance with the assistance of the extraordinary sensing device will be conducted, or a court of general jurisdiction authorized by the state of to issue search warrants.

(4) "Extraordinary sensing device" means an unmanned aircraft system.

(5) "Personal information" means all information that:

(a) 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;

(b) 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

(c) Describes, locates, or indexes anything about a person including, but not limited to, intellectual property, trade secrets, proprietary information, or operational information.

(6)(a) "Sensing device" means a device capable of remotely acquiring personal information from its surroundings, using any frequency of the electromagnetic spectrum.

(b) "Sensing device" does not include equipment whose sole function is to provide information directly necessary for safe air navigation or operation of a vehicle.

(7) "Unmanned aircraft system" means an aircraft that is operated without the possibility of human intervention from within or on the aircraft, together with associated elements, including communication links and components that control the unmanned aircraft that are required for the pilot in command to operate safely and efficiently in the national airspace system.

NEW SECTION. **Sec. 3.** (1) Agency procurement and use of extraordinary sensing devices for surveillance purposes must be conducted in a transparent manner that is open to public scrutiny, as provided in this section.

(2)(a) For the purposes of this section, "governing body" means the council, commission, board, or other controlling body in which legislative powers are vested, except as provided in (b) of this subsection.

(b) For a state agency in which there is no governing body other than the state legislature, "governing body" means the chief executive officer responsible for the governance of the agency.

(3) An agency may not procure an extraordinary sensing device for surveillance purposes without first obtaining explicit approval from the agency's governing body.

(4) The governing body shall develop and make publicly available written policies and procedures for the use of any extraordinary sensing device procured, and provide notice and opportunity for public comment prior to adoption of the written policies and procedures.

NEW SECTION. **Sec. 4.** All operations of an extraordinary sensing device or disclosure of personal information about any person acquired through the operation of an extraordinary sensing device must be conducted in such a way as to minimize the collection and disclosure of personal information not authorized under this chapter.

NEW SECTION. **Sec. 5.** (1) An extraordinary sensing device may be operated and personal information from such operation disclosed in order to collect personal information pursuant to a search warrant issued by a court of competent jurisdiction as provided in this section.

(2) Each petition for a search warrant from a judicial officer to permit the use of an extraordinary sensing device and personal information collected from such operation must be made in writing, upon oath or affirmation, to a judicial officer in a court of competent jurisdiction for the geographic area in which an extraordinary sensing device is to be operated or where there is probable cause to believe the offense for which the extraordinary sensing device is sought has been committed, is being committed, or will be committed.

(3) The law enforcement officer shall submit an affidavit that includes:

(a) The identity of the applicant and the identity of the agency conducting the investigation;

(b) The identity of the individual and area for which use of the extraordinary sensing device is being sought;

(c) Specific and articulable facts demonstrating probable cause to believe that there has been, is, or will be criminal activity and that the operation of the extraordinary sensing device system will uncover evidence of such activity or facts to support the finding that there is probable cause for issuance of a search warrant pursuant to applicable requirements; and

(d) A statement that other methods of data collection have been investigated and found to be either cost prohibitive or pose an unacceptable safety risk to a law enforcement officer or to the public.

(4) If the judicial officer finds, based on the affidavit submitted, there is probable cause to believe a crime has been committed, is being committed, or will be committed and there is probable cause to believe the personal information likely to be

obtained from the use of the extraordinary sensing device will be evidence of the commission of such offense, the judicial officer may issue a search warrant authorizing the use of the extraordinary sensing device. The search warrant must authorize the collection of personal information contained in or obtained from the extraordinary sensing device, but must not authorize the use of a biometric identification system.

(5) Warrants may not be issued for a period greater than ten days. Extensions may be granted, but no longer than the authorizing judicial officer deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days.

(6) Within ten days of the execution of a search warrant, the officer executing the warrant must serve a copy of the warrant upon the target of the warrant, except if notice is delayed pursuant to section 6 of this act.

NEW SECTION. **Sec. 6.** (1) A governmental entity acting under this section may, when a warrant is sought, include in the petition a request, which the court shall grant, for an order delaying the notification required under section 5(6) of this act for a period not to exceed ninety days if the court determines that there is a reason to believe that notification of the existence of the warrant may have an adverse result.

(2) An adverse result for the purposes of this section is:

(a) Placing the life or physical safety of an individual in danger;

(b) Causing a person to flee from prosecution;

(c) Causing the destruction of or tampering with evidence;

(d) Causing the intimidation of potential witnesses; or

(e) Jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a copy of certification.

(4) Extension of the delay of notification of up to ninety days each may be granted by the court upon application or by certification by a governmental entity.

(5) Upon expiration of the period of delay of notification under subsection (2) or (4) of this section, the governmental entity shall serve a copy of the warrant upon, or deliver it by registered or first-class mail to, the target of the warrant, together with notice that:

(a) States with reasonable specificity the nature of the law enforcement inquiry; and

(b) Informs the target of the warrant: (i) That notification was delayed; (ii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and (iii) which provision of this section allowed such delay.

NEW SECTION. **Sec. 7.** (1) It is lawful under this section for any law enforcement officer or other public official to operate an extraordinary sensing device and disclose personal information from such operation if such officer reasonably determines that an emergency situation exists that involves criminal activity and presents immediate danger of death or serious physical injury to any person and:

(a) Requires operation of an extraordinary sensing device before a warrant authorizing such interception can, with due diligence, be obtained;

(b) There are grounds upon which such a warrant could be entered to authorize such operation; and

(c) An application for a warrant providing such operation is made within forty-eight hours after the operation has occurred or begins to occur.

(2) In the absence of a warrant, an operation of an extraordinary sensing device carried out under this section must immediately terminate when the personal information sought is obtained or when the application for the warrant is denied, whichever is earlier.

(3) In the event such application for approval is denied, the personal information obtained from the operation of a device must be treated as having been obtained in violation of this chapter, except for purposes of section 12 of this act, and an inventory must be served on the person named in the application.

NEW SECTION. **Sec. 8.** (1) It is lawful under this section for a law enforcement officer, agency employee, or authorized agent to operate an extraordinary sensing device and disclose personal information from such operation if:

(a) An officer, employee, or agent reasonably determines that an emergency situation exists that:

(i) Does not involve criminal activity;

(ii) Presents immediate danger of death or serious physical injury to any person; and

(iii) Requires operation of an extraordinary sensing device to reduce the danger of death or serious physical injury;

(b) An officer, employee, or agent reasonably determines that the operation does not intend to collect personal information and is unlikely to accidentally collect personal information, and such operation is not for purposes of regulatory enforcement including, but not limited to:

(i) Monitoring to discover, locate, observe, and prevent forest fires;

(ii) Monitoring an environmental or weather-related catastrophe or damage from such an event;

(iii) Surveying for wildlife management, habitat preservation, or environmental damage; and

(iv) Surveying for the assessment and evaluation of environmental or weather-related damage, erosion, flood, or contamination;

(c) The operation is part of a training exercise conducted on a military base and the extraordinary sensing device does not collect personal information on persons located outside the military base;

(d) The operation is for training and testing purposes by an agency and does not collect personal information; or

(e) The operation is part of the response to an emergency or disaster for which the governor has proclaimed a state of emergency under

(2) Upon completion of the operation of an extraordinary sensing device pursuant to this section, any personal information obtained must be treated as information collected on an individual other than a target for purposes of section 11 of this act.

NEW SECTION. **Sec. 9.** An unmanned aircraft system may not be utilized for the purposes of investigation or enforcement of regulatory violations or noncompliance until the legislature has adopted legislation specifically permitting such use.

NEW SECTION. **Sec. 10.** Whenever any personal information from an extraordinary sensing device has been acquired, no part of such personal information and no evidence derived therefrom may be received

in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the state or a political subdivision thereof if the collection or disclosure of that personal information would be in violation of this chapter.

NEW SECTION. **Sec. 11.** Personal information collected during the operation of an extraordinary sensing device authorized by and consistent with this chapter may not be used, copied, or disclosed for any purpose after conclusion of the operation, unless there is probable cause that the personal information is evidence of criminal activity. Personal information must be deleted as soon as possible after there is no longer probable cause that the personal information is evidence of criminal activity; this must be within thirty days if the personal information was collected on the target of a warrant authorizing the operation of the extraordinary sensing device, and within ten days for other personal information collected incidentally to the operation of an extraordinary sensing device otherwise authorized by and consistent with this chapter. There is a presumption that personal information is not evidence of criminal activity if that personal information is not used in a criminal prosecution within one year of collection.

NEW SECTION. **Sec. 12.** Any person who knowingly violates this chapter is subject to legal action for damages, to be brought by any other person claiming that a violation of this chapter has injured his or her business, his or her person, or his or her reputation. A person so injured is entitled to actual damages and reasonable attorneys' fees and other costs of litigation.

NEW SECTION. **Sec. 13.** (1) For any calendar year in which an agency has procured or used an extraordinary sensing device, the agency must prepare an annual report. The report must be made publicly available electronically and must, at a minimum, include the following:

(a) The types of extraordinary sensing devices procured and used, the purposes for which each type of extraordinary sensing device was procured and used, the circumstances under which use was authorized, and the name of the officer or official who authorized the use;

(b) Whether deployment of the device was perceptible to the public;

(c) The specific kinds of personal information that the extraordinary sensing device collected;

(d) The length of time for which any personal information collected by the extraordinary sensing device was retained;

(e) The specific steps taken to mitigate the impact on an individual's privacy, including protections against unauthorized use and disclosure and adoption of a data minimization protocol; and

(f) An individual point of contact for citizen complaints and concerns.

(2)(a) Each agency, except as provided in (b) of this subsection, must submit to the agency's governing body the annual report for the previous calendar year by March 1st, beginning in

(b) In the case of state agencies with no governing body other than the legislature, the annual reports must be filed electronically with the office of financial management, who must compile the results and submit them electronically to the legislature by September 1st of each year, beginning in

NEW SECTION. **Sec. 14.** Sections 2 through 13 of this act are each added to chapter 9.73 RCW and codified with the subchapter heading of "extraordinary sensing devices."

NEW SECTION. **Sec. 15.** If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

--- END ---