
BILL REQUEST - CODE REVISER'S OFFICE

BILL REQ. #: H-2786.1/13

ATTY/TYPIST: ML:lel

BRIEF DESCRIPTION: Regarding technology-enhanced government surveillance.

1 AN ACT Relating to technology-enhanced government surveillance;
2 adding new sections to chapter 9.73 RCW; creating a new section; and
3 prescribing penalties.

4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

5 NEW SECTION. **Sec. 1.** The rapid development of advanced
6 technologies that can monitor and record private behavior beyond the
7 ability of normal human senses has made it necessary for the
8 legislature to establish new technology-neutral standards to protect
9 individual liberty. While all technology is neutral in itself, it is
10 the application by humans that can be both good and bad. Whether
11 surveillance is conducted by the individual, groups, or the government,
12 citizens are not always aware when technology is being used to record
13 and monitor their personal and private behavior. Surveillance
14 conducted remotely and observing activities that were previously not
15 viewable by the naked eye is rapidly increasing. As a consequence,
16 conduct that was formerly considered private may be at risk of losing
17 legal protection from government intrusion--for example, satellites
18 equipped with high resolution cameras can peer into our backyards and
19 our skylights, or read the book we are reading on a park bench. The

1 legislature finds that, while constitutional protections against
2 government invasions into private affairs are strongest inside one's
3 home with the windows shuttered, the scope of legal protections drops
4 precipitously for the private affairs of an individual who leaves his
5 or her home, and for those private affairs of an individual conducted
6 inside the home but from a public vantage point. The legislature finds
7 that the right to privacy protects people, not places, and although the
8 expectation of privacy in public spaces may be lower than in private
9 spaces, it is not entirely eliminated. The legislature finds that when
10 legal protections for personal privacy fail to keep up with evolving
11 technology, the delicate balance of power between an individual and the
12 state may be disturbed in a manner destructive to the personal freedom
13 that is essential to our democracy. It is the intent of the
14 legislature to restore this delicate balance, by establishing an
15 expectation that certain forms of government surveillance using
16 extraordinary sensing devices may not be conducted, from any vantage
17 point, without the supervision of a court, through a court-ordered
18 warrant.

19 NEW SECTION. **Sec. 2.** The definitions in this section apply
20 throughout sections 2 through 9 of this act unless the context clearly
21 requires otherwise.

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

24 (2) "Clear and conspicuous notice" means notice that is reasonably
25 easy to find and easily understandable in terms of content and style to
26 the average reader, informing the public of the form of surveillance
27 used and how the information obtained by the surveillance will be
28 stored, used, or disclosed.

29 (3) "Conduct surveillance" means to engage in or induce a third
30 party to engage in the act of collecting personal information using an
31 extraordinary sensing device.

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

1 (5) "Extraordinary sensing device" means a sensing device that is
2 uncommon to society, under a community-based standard, such that its
3 use and existence has not become integrated into the ordinary societal
4 experience of the community as of the effective date of this section.
5 In making a determination about whether a device is uncommon and has
6 not been socially integrated into the experience of a community, the
7 court shall consider all relevant factors including, but not limited
8 to:

9 (a) The level of technology and sophistication of the device;

10 (b) The extent to which the device is commercially available to
11 individual members of the community, as of the effective date of this
12 section;

13 (c) The extent of the use of the device in a nongovernmental
14 context within the community and public awareness in the community of
15 such use;

16 (d) The extent to which the device makes conduct visible from an
17 extraordinary vantage point; and

18 (e) The amount of time in which the technology has been in
19 existence as of the effective date of this section.

20 (6) "Extraordinary vantage point" means a vantage point to which an
21 ordinary member of the public would not have ready access.

22 (7) "Imperceptible" means highly unlikely to be perceived by the
23 unassisted senses of a human being of ordinary abilities.

24 (8) "Personal information" means all information that:

25 (a) Describes, locates, or indexes anything about a person
26 including, but not limited to, his or her social security number,
27 driver's license number, agency-issued identification number, student
28 identification number, real or personal property holdings derived from
29 tax returns, and the person's education, financial transactions,
30 medical history, ancestry, religion, political ideology, or criminal or
31 employment record;

32 (b) Affords a basis for inferring personal characteristics, such as
33 finger and voice prints, photographs, or things done by or to such a
34 person; and the record of the person's presence, registration, or
35 membership in an organization or activity, or admission to an
36 institution; or

37 (c) Describes, locates, or indexes anything about a person

1 including, but not limited to, intellectual property, trade secrets,
2 proprietary information, or operational information.

3 (9) "Sensing device" means a device capable of remotely acquiring
4 data or remotely sensing information from its surroundings, using any
5 frequency of the electromagnetic spectrum, including but not limited to
6 wireless devices operating in infrared, visible, ultraviolet, and
7 acoustic frequencies, devices using chemical or biological detectors,
8 devices using biometric and genetic technology, and radiation gauges.

9 NEW SECTION. **Sec. 3.** Except as otherwise specifically authorized
10 in this section and sections 4 through 6 of this act, it is unlawful
11 for the state of Washington, its agencies, and political subdivisions
12 to conduct surveillance that is imperceptible to a person whose
13 personal information may be collected by an extraordinary sensing
14 device, when:

15 (1) The persons or activities being observed are located within the
16 boundaries of an individual's home and curtilage, and the surveillance
17 is conducted without the consent of the individual or individuals
18 entitled to privacy in that place; or

19 (2) The persons or activities being observed are located in a
20 public space and clear and conspicuous notice of the surveillance has
21 not been posted.

22 NEW SECTION. **Sec. 4.** (1) The state of Washington, its agencies,
23 and political subdivisions may conduct surveillance otherwise
24 prohibited under section 3 of this act pursuant to a criminal search
25 warrant issued by a court of competent jurisdiction upon a finding of
26 probable cause.

27 (2) Evidence obtained in violation of sections 2 through 9 of this
28 act may not be used to support a finding of probable cause under this
29 section.

30 (3) Except as provided in section 8 of this act, no personal
31 information collected on an individual or area other than the target
32 that justified the issuance of the search warrant may be used, copied,
33 or disclosed for any purpose. This personal information must be
34 deleted as soon as possible, and in no event later than ten days after
35 collection.

1 NEW SECTION. **Sec. 5.** (1) It is lawful for an agency employee or
2 authorized agent to conduct surveillance and disclose personal
3 information derived from operation of an extraordinary sensing device
4 if:

5 (a) The person is acting under the direction of an agency elected
6 official, appointed official, director, or deputy director, and the
7 official or director reasonably determines that an emergency situation
8 exists that involves criminal activity and presents immediate danger of
9 death or serious physical injury to any person and:

10 (i) Addressing the danger requires operation of the device before
11 a warrant authorizing the operation can, with due diligence, be
12 obtained;

13 (ii) There are grounds upon which such a warrant could be entered
14 to authorize such an operation; and

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

18 (b) The agency employee or public official reasonably determines
19 that an emergency situation exists that does not involve criminal
20 activity, presents an immediate danger of death or serious physical
21 injury to any person, and requires operation of an extraordinary
22 sensing device to reduce the danger of death or serious physical
23 injury, and:

24 (i) The agency employee or public official reasonably determines
25 that the operation does not intend to collect personal information and
26 is unlikely to accidentally collect personal information; or

27 (ii) The operation is part of a training exercise conducted on a
28 military base and the ~~public unmanned aircraft system~~ does not collect
29 personal information on persons located outside the military base.

30 (2) Surveillance conducted using an extraordinary sensing device in
31 the absence of a warrant under the authority of this section must be
32 immediately terminated when the personal information sought is obtained
33 or when the application for the warrant is denied, whichever is
34 earlier.

35 (3) Any law enforcement or other agency that conducts surveillance
36 under the authority of this section must issue an annual public report
37 indicating:

1 (a) The purposes for which an extraordinary sensing device was
2 used;

3 (b) The circumstances under which use was authorized, including the
4 name of the officer or official who authorized the use;

5 (c) The specific kinds of personal information that the
6 extraordinary sensing devices have collected about individuals;

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

9 (e) The specific steps taken to mitigate the impact on an
10 individual's privacy, including protections against unauthorized use
11 and disclosure; and

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

14 (4) In the event an application for a warrant under subsection
15 (1)(a)(iii) of this section is denied, the personal information
16 obtained from the operation of an extraordinary sensing device must be
17 treated as having been obtained in violation of this chapter for the
18 purpose of the exclusion of evidence under section 4(2) of this act.

19 NEW SECTION. **Sec. 6.** For the purpose of regulatory enforcement of
20 a permitted or licensed activity, it is lawful for the state of
21 Washington, its agencies, and political subdivisions to conduct
22 surveillance and disclose personal information collected with the
23 assistance of an extraordinary sensing device only as specifically
24 authorized in this section.

25 (1)(a) The agency must have given the permittee or licensee clear
26 and conspicuous notice at the time that the permit or license was
27 granted or renewed that the permitted or licensed activity could be
28 subject to such surveillance; and

29 (b) All government surveillance conducted with the assistance of an
30 extraordinary sensing device must be conducted in such a way as to
31 minimize the collection and disclosure of personal information not
32 authorized under this chapter.

33 (2) Prior to conducting surveillance under the authority of this
34 section, the agency must have adopted and published a data minimization
35 protocol establishing reasonable measures to ensure that the
36 surveillance is unlikely to accidentally collect and retain personal

1 information of individuals or activities not related to the permitted
2 or licensed activity. The data minimization protocol must state the
3 steps taken by the agency to ensure that:

4 (a) Personal information is collected for legitimate, limited, and
5 specific stated purposes;

6 (b) Collection of personal information is limited to the minimum
7 amount necessary for the specified purposes and appropriate
8 technologies are used to minimize the data collected. For example, the
9 agency uses encryption where practicable to obscure the images of
10 individuals whose identity is not related to the regulatory purpose of
11 the surveillance;

12 (c) Personal information is only used and disclosed for the
13 purposes specified;

14 (d) Personal information is deleted pursuant to precise and
15 appropriately limited retention schedules and in such a manner that
16 prevents the agency or a third party from being able to reconstruct the
17 personal information after deletion; and

18 (e) Only authorized persons have access to information and data
19 obtained through the surveillance and authorized persons have received
20 training on their duties and obligations to ensure the confidentiality
21 of the information and data.

22 NEW SECTION. **Sec. 7.** (1) An ex parte order authorizing the
23 conduct of surveillance with the assistance of an extraordinary sensing
24 device may be issued by any superior court judge in the state upon
25 verified application of either the state attorney general or any county
26 prosecuting attorney setting forth fully facts and circumstances upon
27 which the application is based and stating that:

28 (a) There are reasonable grounds to believe that national security
29 is endangered, that a human life is in danger, that arson is about to
30 be committed, or that a riot is about to be committed;

31 (b) There are reasonable grounds to believe that evidence will be
32 obtained that is essential to the protection of national security, the
33 preservation of human life, or the prevention of arson or a riot; and

34 (c) There are no other means readily available for obtaining such
35 information.

36 (2) Where statements are solely upon the information and belief of
37 the applicant, the grounds for the belief must be given.

1 (3) The applicant must state whether any prior application has been
2 made to obtain prior authorization to use an extraordinary sensing
3 device to observe private conduct of the same person or in the same
4 location. If a prior application exists, the applicant shall disclose
5 the current status thereof.

6 (4) The application and any order issued under this section must
7 identify as fully as possible the particular surveillance technology
8 with which the information is to be obtained and the purpose thereof.

9 (5) The court may examine upon oath or affirmation the applicant
10 and any witness the applicant desires to produce or the court requires
11 to be produced.

12 (6) Orders issued under this section are effective for fifteen
13 days, after which period the court that issued the order may upon
14 application of the officer who secured the original order renew or
15 continue the order for an additional period not to exceed fifteen days.

16 (7) No order issued under this section may authorize or purport to
17 authorize any activity that would violate any laws of the United
18 States.

19 NEW SECTION. **Sec. 8.** Any information obtained in violation of
20 sections 3 through 7 of this act is inadmissible in any civil or
21 criminal case in all courts of general or limited jurisdiction in this
22 state, except:

23 (1) In an action for damages under section 9 of this act, with the
24 permission of the person whose rights have been violated; or

25 (2) In a criminal action in which the defendant is charged with a
26 crime, the commission of which would jeopardize national security.

27 NEW SECTION. **Sec. 9.** Any person who violates the provisions of
28 sections 2 through 8 of this act is subject to legal action for
29 damages, to be brought by any other person claiming that a violation of
30 sections 2 through 8 of this act has injured his or her business, his
31 or her person, or his or her reputation. A person so injured is
32 entitled to actual damages, including mental pain and suffering endured
33 by the person on account of a violation of the provisions of sections
34 2 through 8 of this act, or liquidated damages computed at the rate of
35 one thousand dollars per day for each day of violation, not to exceed

1 ten thousand dollars, and reasonable attorneys' fees and other costs of
2 litigation.

3 NEW SECTION. **Sec. 10.** Sections 2 through 9 of this act are each
4 added to chapter 9.73 RCW and codified with the subchapter heading
5 "extraordinary sensing devices."

6 NEW SECTION. **Sec. 11.** If any provision of this act or its
7 application to any person or circumstance is held invalid, the
8 remainder of the act or the application of the provision to other
9 persons or circumstances is not affected.

--- END ---