S-3756.1

SENATE BILL 6432

State of Washington 61st Legislature 2010 Regular Session

By Senators Kline, Regala, and Kohl-Welles

Read first time 01/14/10. Referred to Committee on Judiciary.

AN ACT Relating to enhanced intelligence in Washington state; adding a new chapter to Title 42 RCW; and prescribing penalties.

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

NEW SECTION. **Sec. 1.** POLICY. Whereas free discourse is essential to a functioning democracy, the legislature declares it is the policy of Washington state that an individual or group may not be subject to collection, maintenance, or dissemination of information about the individual or group's political or religious beliefs or activities, absent a reasonable suspicion of criminal conduct.

NEW SECTION. **Sec. 2.** SHORT TITLE. This chapter may be known and cited as the Washington enhanced intelligence act.

NEW SECTION. **Sec. 3.** DEFINITIONS. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Collect" or "collection" means to preserve in tangible form, including temporary or permanent storage by electronic means, information as a record or file of an intelligence data entity, which

is directly or indirectly retrievable by intelligence data entity personnel. "Collect" or "collection" does not include making personal notes which are not retrievable by other intelligence data entity personnel.

(2) "Intelligence data entity" means any state or local government entity, or any entity in which any segment of the state or local government is a partner, that collects, analyzes, and shares information for law enforcement, public safety, or antiterrorism purposes.

(3) "Protected information" means information about the political, religious, or social views, associations, or activities of any individual, group, association, organization, corporation, partnership, limited liability company, or other business. "Protected information" does not include materials disseminated to the public by a government entity.

NEW SECTION. **Sec. 4.** COLLECTING PROTECTED INFORMATION. (1) An intelligence data entity may not collect or maintain protected information unless:

(a) The information directly relates to an investigation of criminal activities;

(b) There is reasonable suspicion that the subject of the information is or may be involved in criminal conduct; and

(c) The entity has made reasonable efforts to exhaust alternative means.

(2) Any investigation based on protected information, or which is used to justify the collection or maintenance of protected information, must be authorized in writing by the executive authority of the relevant intelligence data entity before the investigation begins or, if prior written authorization is not possible, within five days after the investigation begins. This written authorization must specify why collection or maintenance of protected information is necessary. A record of this written authorization, including the reasons for its necessity, must be kept and maintained for a minimum of five years after the investigation is closed.

NEW SECTION. **Sec. 5.** INFORMATION SHARING. (1) Except where

required by federal law, an intelligence data entity may not disseminate or accept protected information unless:

(a) The executive authority of the originating intelligence data entity reviews and authorizes the dissemination in writing before the dissemination or acceptance occurs or, if prior written authorization is not possible, within five days after the dissemination or acceptance occurs. The intelligence data entity shall retain a record of this written authorization for a minimum of five years;

(b) The collecting and receiving agencies comply with this statute; and

(c) The originating entity records each instance of dissemination in a log, containing the name of the subject or subjects and the name of the entity with whom the subject or subjects' information was shared.

(2) An intelligence data entity that has disseminated protected information is exempt from this section if:

(a) The protected information is disseminated to an individual or group requesting the individual or group's own information;

(b) The protected information is requested by a third party with the consent of the individual or group that is the subject of the information; or

(c) The dissemination was required by state or federal law.

NEW SECTION. **Sec. 6.** INTERNAL REVIEW. (1) At least once every three years, intelligence data entities shall conduct an internal audit, the results of which must be publicly available. This audit must include:

(a) The number of investigations authorized under section 4(2) or 5(1)(a) of this act that remain open;

(b) The length of time open investigations authorized under section 4(2) or 5(1)(a) of this act have remained open;

(c) For each open investigation authorized under section 4(2) or 5(1)(a) of this act, a justification for continued collection or maintenance of protected information;

(d) Since the last audit, the number of investigations for which authorization under section 4(2) or 5(1)(a) of this act was denied;

(e) Since the last audit, the number of authorized disseminations

under section 5(1) of this act, and to which entity each dissemination was made;

(f) Since the last audit, the number of investigations authorized under section 4 of this act that have been closed; and

(g) Certification by the head of the investigating authority or intelligence data entity that all protected information collected, stored, or maintained complies with this chapter.

(2) All state or local intelligence data entities shall review all protected information recorded in any investigation file during each audit. All intelligence data entities shall immediately destroy protected information that is not accurate or relevant to an ongoing criminal investigation. The intelligence data entity shall make reasonable efforts to ensure the accuracy of protected information.

(3) The intelligence data entity shall retain documents related to the authorization and termination of investigations based wholly or partially on protected information collected pursuant to section 4 of this act, and any authorization to disseminate protected information pursuant to section 5(1)(c) of this act.

NEW SECTION. **Sec. 7.** REQUESTS FOR INFORMATION. Unless the requester is the subject of an open investigation authorized under section 5(2) of this act, an individual about whom protected information was collected or disseminated has a right to the following from any intelligence data entity:

(1) To request and receive any protected information that has been collected in which he or she is included or referenced;

(2) To request and receive any dissemination log, as required by section 5(1)(c) of this act, listing with whom his or her protected information has been shared, accessed, or disseminated;

(3) To require destruction of all protected information that is not directly related to an ongoing, authorized investigation; and

(4) To require destruction of requester's protected information by any recipients.

NEW SECTION. **Sec. 8.** INTELLIGENCE AUDITOR. (1) The state auditor shall monitor compliance with sections 4 through 7 of this act.

(2) The auditor shall conduct an in-place audit of intelligence data entity files and records at unscheduled intervals. The

intelligence data entity shall provide temporary space for the auditor to conduct the audit in secure areas close to the records to be reviewed.

(3) The auditor shall publish a report containing a general description of the files and records reviewed and a discussion of any substantial violation of this chapter discovered during the audit.

NEW SECTION. **Sec. 9.** CIVIL LIABILITY. (1) An agency or entity that fails to comply with any requirement imposed under this title with respect to any person or group is liable to that person or group in an amount equal to the sum of any actual damages sustained by the injured party as a result of the failure, or statutory damages of not less than one hundred dollars and not more than one thousand dollars; and, in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorneys' fees as determined by the court.

(2) On a finding by the court that an unsuccessful pleading, motion, or other paper filed in connection with an action under this section was filed in bad faith or for purposes of harassment, the court shall award to the prevailing party attorneys' fees reasonable in relation to the work expended in responding to the pleading, motion, or other paper.

NEW SECTION. **Sec. 10.** Sections 1 through 9 of this act constitute a new chapter in Title 42 RCW.

--- END ---