SENATE BILL REPORT
SB 6432

As of January 25, 2010

Title: An act relating to enhanced intelligence in Washington state.

Brief Description: Creating the Washington enhanced intelligence act.

Sponsors: Senators Kline, Regala and Kohl-Welles.

Brief History:
Committee Activity: Judiciary: 1/20/10.

SENATE COMMITTEE ON JUDICIARY

Staff: Kim Johnson (786-7472)

Background: Various state and local government entities collect, analyze, and share information for law enforcement, public safety, or antiterrorism purposes. Other than the Public Records Act, there is generally no specific overarching state statute requiring oversight or approval of the collection and dissemination of this type of information.

Depending on the type of information collected and the purpose for which it was collected, federal laws may apply. For example, the collection and dissemination of intelligence information gathered by state and local law enforcement entities participating under the Omnibus Crime Control and Safe Streets Act of 1968, is subject to the requirements of the Criminal Intelligence Systems Operating Policies as set out in 28 CFR Part 23. These policies specify what type of information may be collected; whether a reasonable suspicion of criminal activity is required; how long the information is to be maintained; and whether the information may shared; etc. Additionally, individual agency operating procedures may be in place to guide agency collection, use, and dissemination.

Summary of Bill: Protected information is defined as 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.

Intelligence gathering entity is defined as any state or local government entity or its partner that collects, analyzes, and shares information for law enforcement, public safety or antiterrorism purposes.

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.

Collection of Protected Information. In order for an intelligence gathering entity to collect and maintain protected information the following conditions must be met: (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. Any investigation based on protected information must be authorized in writing by the executive authority of the relevant intelligence data entity before the investigation begins. 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.

Dissemination of Protected Information. Except when required by federal law, an intelligence data entity may not disseminate or accept protected information unless: the executive authority of the originating intelligence data entity reviews and authorizes the dissemination in writing; the collecting and receiving agencies comply with this statute; and the originating entity records each instance of dissemination in a log.

A person or group may request and receive their own information and may also provide consent for a third party to receive the information.

Audit Requirements. At least once every three years, intelligence data entities must conduct an internal audit, the results of which must be publicly available. Criteria for the audit is specified. All state or local intelligence data entities must review all protected information recorded in any investigation file during each audit. All intelligence data entities must immediately destroy protected information that is not accurate or relevant to an ongoing criminal investigation.

Additionally, the State Auditor must monitor compliance with this act and conduct an in-place audit of intelligence data entity files and records at unscheduled intervals. The State Auditor must publish a report containing a general description of the files and records reviewed and a discussion of any substantial violation.

Civil Liability An agency or entity that fails to comply with the requirements imposed under this act is liable to the person or group in an amount equal to the sum of any actual damages sustained by the injured party, or statutory damages of not less than $100 and not more than $1,000; and reasonable attorneys' fees and costs. If a court finds that a pleading, motion or paper filed in connection with an action under this section was filed in bad faith or for purposes of harassment, the court must award to the prevailing party attorneys' fees related to the work expended in responding to the pleading, motion, or paper.

Appropriation: None.

Fiscal Note: Requested on January 14, 2010.

Committee/Commission/Task Force Created: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony: PRO: Since 9/11, intelligence gathering and sharing has changed dramatically. In Washington a system was developed called WAJAC and all intelligence data went into a central processing unit at FBI in Seattle. What we learned was that most of the groups being targeted were involved in peaceful protest activities practicing their first amendment free speech rights. We are not looking to take away from valid law enforcement tools. If we allow the collection of too much information you take away from the police's ability to focus on actual crimes and important information gets lost in the volume. I was co-counsel for ACLU on some of the larger cases against the federal government involving wire tapping. The federal government has an insatiable appetite to collect data on people. Law enforcement agencies in Washington are spying on citizens in Washington who are not suspected of any criminal activity. Too much information and lack of focus on actual criminals leads to vital information slipping through the cracks. The wrong message is sent to lawful citizens who are subject to unnecessary surveillance activities.

I am a past victim of police surveillance in Seattle in the 1970s. I've organized major marches for years in this state and in Washington D.C. Information about me followed me across the country. Years later when my daughter was going to school I met another child's father who said that he had seen me before ... through a scope, during a protest. That kind of surveillance puts a cold blanket over the people who need to be able to exercise their first amendment rights to better their circumstances.

CON: You all ask us to do a very hard job: to protect us all from harm. When we do it well we don't hear about it. When we make a mistake we're never allowed to live it down. What information and activities are actually covered under this act? It is very broad, it covers everything. It applies to everyone. The code of federal regulations already require a criminal nexus and if we can't meet that requirement then we don't collect or maintain that information. The net effect of this bill is that we would lose all federal dollars and federal information. Under this act your partners must agree to abide by this state law. The federal government will not comply with this state law. The cost to review is going to be sufficient. Finally, the code of federal regulations specifically prohibit non-law enforcement personnel from viewing intelligence information which is in direct conflict with the audit requirements laid out in this bill.

OTHER: We have some questions regarding the definitions. The internal review processes may also contradict the federal law and the investigation timelines may prove too restrictive. We currently operate under 30 days. The bill specifies five days. Classifications assigned to types of information could also cause us some difficulties when trying to meet the requirements under this bill. The Washington State correctional system contains 15 adult prisons and a wide range of offenders, with thousands incarcerated. Safety is one of our top concerns and in order to guarantee safety we collect information in a broad number of ways. This bill would hinder our ability to collect information and monitor those incarcerated. We would request an exception for inmates in hard custody.

Persons Testifying: PRO: Tim Smith, Bill of Rights Defense; Juan Bocanegra, EI Comite; Brian Alseth, ACLU; Randy Gainer, citizen.

CON: Don Pierce, Washignton Association of Sherriffs & Police Chiefs.

OTHER: Dan Pachollce, Department of Corrections; Tim Braniff, Scott Jarmon, Washington State Patrol.