# HOUSE BILL REPORT
# SHB 2416

**As Passed House:**
February 16, 2002

**Title:** An act relating to terrorism investigations pursuant to the privacy act.

**Brief Description:** Authorizing additional investigative tools to deter terrorism.

**Sponsors:** By House Committee on Select Committee on Community Security (originally sponsored by Representatives Hurst, Lisk, O'Brien, Ballasiotes, Buck, Kirby, Lovick and Haigh).

**Brief History:**
**Committee Activity:**
Select Committee on Community Security: 1/23/02, 1/31/02 [DPS].
**Floor Activity:**
Passed House: 2/16/02, 77-21.

**Brief Summary of Substitute Bill**

- Provides new and expanded authority under the state's Privacy Act for gathering evidence in terrorism investigations.
- Provides for the sharing, use and admissibility of evidence gathered in terrorism investigations by local, state, and federal investigative and law enforcement officers.

## HOUSE COMMITTEE ON SELECT COMMITTEE ON COMMUNITY SECURITY

**Majority Report:** The substitute bill be substituted therefor and the substitute bill do pass. Signed by 15 members: Representatives Hurst, Chair; Simpson, Vice Chair; Lisk, Ranking Minority Member; Ballasiotes, Barlean, Benson, Buck, Campbell, Haigh, Jackley, Kessler, Morris, O'Brien, Schmidt and Schual-Berke.

**Staff:** Bill Perry (786-7123).

**Background:**

The recent terrorist attacks on this country have heightened debate on issues related to the gathering of evidence by government officials seeking to solve or prevent crimes of

terrorism.

Both state and federal statutes regulate the process by which government may intercept or record private conversations or communications. Beginning in the late 1960s Congress passed comprehensive "eavesdropping" and "wiretap" laws partly in response to U.S. Supreme Court decisions on surveillance practices under broadly written state statutes. The bulk of the current federal law on intercepting private communications was passed as part of the Omnibus Crime Control and Safe Streets Act of 1968. The Washington State Privacy Act was passed in 1970 and has been amended several times since. The state law was, and remains, one of the most restrictive on government surveillance in the country. It is significantly more restrictive than the federal law in several ways.

*(Note: For purposes of economy, throughout this report the term "communication" generally is used to include face to face oral conversation as well as wire, telephonic or electronic communication, and the term "interception" is used to include not only listening in on or otherwise capturing a communication, but also the recording or transmitting of the communication.)*

**Basics Of The State Privacy Act.**

The basic premise of the state Privacy Act is that no private communication may be intercepted without the consent of all of the parties to the communication. It is generally a crime for anyone, government official or private person, to intercept a private communication without everyone's consent. Exceptions to this general rule are provided for in several instances, each with its own set of procedural requirements. These exceptions include:

- With prior judicial authorization, the police may intercept a communication without the consent of any party if there are reasonable grounds to believe evidence will be obtained that is essential to the protection of national security, the preservation of human life, or the prevention of arson or riot. (This provision has rarely, if ever, been used, for reasons discussed below in the comparison with federal law.)

- If at least one party to a communication has consented, the police may get prior judicial authorization for an interception upon a showing of probable cause that the communication will reveal evidence of a felony.

- If at least one party to a communication has consented and there is probable cause to believe the communication involves a drug law violation, then the police may authorize an interception themselves so long as they seek judicial review of the authorization within 15 days afterwards.

- The police may seek prior judicial authorization to install a pen register or trap and trace device to capture the phone numbers of calls going to or coming from a phone, if there is probable cause to believe the use of the register or device will lead to

evidence of a crime.

- Department of Corrections personnel may intercept inmate communications. However, the statute provides that in order to "safeguard the sanctity of the attorney-client privilege" the department may not intercept an inmate's communication with his or her attorney.

- There are several other exceptions in the Privacy Act, such as those related to emergency calls to police or fire officials, harassing or threatening phone calls, and the internal operations of telecommunications providers.

- Law enforcement agencies and courts are required to report to the Administrator for the Courts on a variety of activities related to the Privacy Act.

**The State Privacy Act Is More Restrictive Than The Federal Law.**

The state Privacy Act is more restrictive than the federal law in several ways, including the following:

- Under the state law, evidence obtained from a communication in which no party consented to the interception is generally inadmissible. *Even if lawfully obtained under the Privacy Act*, the evidence is still inadmissible unless the case involves a crime that might "jeopardize national security." Also, the Privacy Act's list of crimes for which a judicial order may be sought in a no-party consent situation is much shorter than the list under the federal law. On the other hand, the lack of showings required in an application under the state law probably makes it unusable even if the inadmissibility provision were removed. For instance, the Privacy Act does not require the police to identify the basis for a requested interception, or to identify their proposed targets or methods, with as much specificity as is required under the federal law. The state law also does not require the court to make any particular findings. For these reasons, at least, no-party consent court orders are apparently never sought under the state law.

- There is no equivalent to the Privacy Act's one-party consent restrictions in federal statute. Generally, under the federal statute if one party to a communication consents to its interception, no further authorization is required. Under the Privacy Act, however, in most one-party consent cases prior judicial authorization is required, and in drug cases, post-interception review is required.

- The Privacy Act's pen register and trap and trace provisions are more restrictive in at least two ways. First, the state law applies only to phones. The federal law is broad enough also to allow the capture of e-mail addresses. Second, under the state law, before the police can get the required judicial authorization they must show there is probable cause to believe use of the register or device will lead to evidence of a crime. Under the federal law, however, the police need only certify to a judge that information likely to be obtained is relevant to an ongoing criminal investigation.

- The Privacy Act's exemption allowing monitoring of inmates contains a prohibition against monitoring an inmate's communications with his or her attorney. Recently adopted federal Department of Justice rules, on the other hand, expressly allow the monitoring of attorney-client communications where the attorney general or other government official has determined the monitoring is necessary to deter future acts of violence or terrorism. Under the federal rule, "privilege teams" consisting of personnel not involved in an inmate's prosecution, are to be used to insure that truly privileged information is not revealed to investigators or prosecutors in the inmate's case. Under the rule, unless the privilege team determines that acts of violence or terrorism are imminent, monitored information may not be disclosed without approval from a federal judge.

- The state supreme court has interpreted the Privacy Act to prohibit federal investigators from testifying in state court about communications intercepted in compliance with federal law if the interception is not also in compliance with the Privacy Act. For example, under federal law no prior judicial authorization is required for the interception of a conversation when at least one party to the conversation has consented to the interception. Such an interception, however, violates the Privacy Act's requirement of prior judicial authorization (or judicial review, in the case of drug crimes), and therefore such evidence intercepted by federal officers is inadmissible in state court.

---

**Summary of Substitute Bill:**

Various changes are made to the state's Privacy Act. In all instances, the changes authorizing the interception of communications are limited to cases involving acts of terrorism.

An act of terrorism– is defined as the commission, or conspiracy to commit, any of the following crimes:
- Terrorism in the first degree;
- Terrorism in the second degree;
- Unlawful use or possession of a weapon of mass destruction; or
- Threatening acts of terrorism in the first degree.

**No-Party Consent Cases.**
A new provision is added to the Privacy Act to allow for prior judicial authorization to intercept a communication involving acts of terrorism when no party to the communication has consented to the interception. The provision follows closely the federal law, except that the provision is limited to cases involving terrorism.

The state attorney general or a county prosecutor may authorize a law enforcement agency to apply to a superior court for authorization for an interception. The application

must include, among other things:

- The identity of the applicant;
- A full and complete statement of the facts and circumstances relied upon for the application including;
    - Details of the particular crime in question;
    - Particular description of the nature and location of the proposed facilities or places where the interception is to occur (with exceptions summarized below);
    - Particular description of the type of communication involved; and
    - The identity of the suspect, if known.
    - A full and complete statement whether other methods have been tried and have failed or are too dangerous to try;
    - The length of time of the proposed interception; and
    - A full and complete statement of facts regarding all previous applications involving the same suspects, facilities or places.

The court may authorize the interception if it determines that normal investigative procedures have been tried and have failed or are too dangerous to try, and that there is probable cause to believe that:

- A person is, has, or will commit an act of terrorism;
- Particular communications concerning that act of terrorism will be obtained by the interception;
- The facilities or place from which the interception is to occur is used by the suspect (with exceptions summarized below).

The court's order of authorization is to contain information based on the application and the court's determinations, and is valid until the objective of the application is achieved, but in no event for longer than 30 days. Extensions of 30 days may be had upon reapplication. The order may require periodic progress reports. Any recordings must be made in a way that protects against editing, and must be delivered to the court for sealing. Applications and orders also are to be sealed. The sealed items must be kept for at least 10 years.

Unless the government makes a showing of good cause and obtains a postponement, not more than 90 days after an order expires, the court is to make an "inventory" indicating that an order was entered, what the period of authorization was, and whether interceptions were made. This inventory is to be served on the person named in the order. Procedures are also supplied for notification of parties before trial and for motions to suppress evidence based on non-compliance with the act.

As noted above, exceptions are provided to the requirement of specifying certain information in the application, and of including similar information in the court's determination to order an interception. Ordinarily, the application and the court order must provide a specific description of the location and nature of the facilities or places from which an interception is to occur. The exceptions to this normal rule apply as follows:

- In the case of an oral communication, the specification requirement does not apply if the application identifies the suspect and contains a full and complete statement as to why specification is not practical, and the court finds specification is not practical;

- In the case of a wire or electronic communication, the specification requirement does not apply if the application identifies the suspect and the court finds that the applicant has shown there is probable cause to believe the suspect's actions could have the effect of thwarting the interception from a specified facility. An authorization under this exception must be limited to the time it is reasonable to presume the suspect will be reasonably near the instrument through which the communication is to be transmitted.

**One-Party Consent Cases.**

A new provision is added to the Privacy Act to allow law enforcement agencies to authorize the interception of communications with post-interception judicial review when at least one party has consented to the interception and the communication involves an act of terrorism. This provision is patterned on the existing Privacy Act section relating to one-party consent cases involving drug crimes.

The chief law enforcement officer or specified designee of an agency can authorize an interception of a communication related to terrorism if:

- At least one party to the communication has consented to the interception;

- There is probable cause to believe the communication will concern an act of terrorism; and

- The officer completes a report that identifies the required probable cause; the authorizing and consenting parties and the suspect; the details of the suspected offense; the time and location of the communication; and whether prior judicial

authorization has been sought.

These authorizations are good for 24 hours, with no more than two extensions.

If an interception occurs, the law enforcement agency must report to the court within 15 days after the authorization was made. Within two days after that, the court is to review the authorization to see if it met the requirements described above. If the court invalidates the authorization it is to order the destruction of any recordings or copies of the interception. If the court has determined that probable cause did not exist for the authorization, within six months of that determination any nonconsenting party to the intercepted communication is to be notified of the interception. The notice must include information on when, where, and by whom the interception was performed. An authorizing agency may seek six-month extensions of this notice requirement on the grounds that the notice might jeopardize an ongoing investigation.

An intentional interception done in violation of the one-party consent interception requirements is a class C felony. In addition, a law enforcement agency may be liable for civil damages, including exemplary damages of $25,000, if the agency authorized the interception without the required probable cause and without a reasonable suspicion that the intercepted communication would involve the act of terrorism identified in the authorization.

**Pen Registers And Traps And Traces.**
A new provision is added to the Privacy Act to allow the expanded use of pen registers and traps and traces in investigations of terrorism. This provision is based on the existing Privacy Act section allowing the use of pen registers and traps and traces on telephones. However, this new provision regarding terrorism has expanded definitions that are taken from the federal law and that also cover electronic communications such as e-mail.

For purposes of terrorism investigations, a pen register is a device that obtains dialing, routing, addressing, or signaling information from an instrument or facility from which an outgoing electronic communication is transmitted, but that does not capture the contents of the communication. A trap and trace is a device or process that captures incoming dialing, routing, addressing or signaling information that is reasonably likely to identify the source of the communication, but that does not capture content.

An investigative or law enforcement officer may seek authorization from the superior court to use a pen register or a trap and trace. The court is to authorize the use if it finds there is probable cause to believe the use will lead to evidence of terrorism. The court's order must specify the suspect, if known, and the person who owns or uses the instrument or facility to which the device or process is to be attached or applied. It must also specify the attributes of the communication to which the order applies, including, if known, the location of the instrument or facility. The order must also specify the

geographic limits of any authorization for the use of a trap and trace. An order is valid for not more than 60 days, after which an additional 60 days may be sought. Any additional extension, beyond the first extension, requires a showing of "high probability" that evidence sought is "much more likely" to be obtained under the extension and a showing that there are extraordinary circumstances such as an immediate danger of death to a law enforcement officer.

The court's order may require the provider of a communications facility to assist in the use of the pen register or trap and trace. The provider is to be reasonably compensated for the assistance. Good faith reliance by the provider on an order is a complete defense to any criminal or civil action based on the provider having supplied assistance or information.

In an emergency situation, a law enforcement agency may proceed before getting judicial authorization. To do so, the agency and the prosecuting attorney must jointly determine that there is probable cause to believe there is immediate danger of death or serious injury, that there is not enough time to get a court order, but that there are grounds to get such an order if time permitted. Failure to seek a court order within 48 hours of the emergency installation or use of a pen register or trap and trace is a gross misdemeanor.

**Sharing And Use Of Evidence Obtained.**

A new provision is added to the Privacy Act detailing the ways in which law enforcement agencies may share and use information obtained through surveillance authorized in investigations of terrorism.

- Federal law enforcement officers are expressly given authority to testify in state court as to evidence of terrorism obtained pursuant to federal law, if the evidence was obtained with prior judicial authorization.

- Federal or state officers may use or share information lawfully obtained under the terrorism provisions of the Privacy Act if the use or sharing is appropriate to their duties.

- Any person who has lawfully received information under the terrorism provisions of the Privacy Act may testify as to that information in a state court.

- Evidence of a crime other than terrorism may also be shared or used if the evidence was obtained lawfully during a terrorism surveillance authorized under the terrorism provisions of the Privacy Act. Such evidence of another crime may be testified to in state court upon a showing that it was obtained in accordance with the surveillance authorization.

- State officers are authorized to disclose to federal officials any evidence of foreign intelligence or counterintelligence obtained during a lawful surveillance under the

terrorism provisions of the Privacy Act.

- The interception of a communication does not change the nature of any privileged information in that communication.

**Miscellaneous Provisions.**
Various terms are defined for purposes of surveillance of terrorism under the Privacy Act.

With respect to the new terrorism provisions of the Privacy act, the state attorney general is given the same concurrent authority with county prosecutors as already exists with respect to other provisions of the Privacy Act.

---

**Appropriation:** None.

**Fiscal Note:** Not Requested.

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

**Testimony For:** There is a real threat of terrorism in this state. The current Privacy Act presents substantial obstacles to cooperative investigations between state and federal law enforcement agencies. This bill will do a great deal to facilitate much needed cooperative efforts. The federal government lacks the personnel and resources to adequately respond to the threat of terrorism without help from state and local officials. Current inadequacies in the Privacy Act make it unusable as an investigative tool, but at the same time often prevent information lawfully obtained under federal laws from being used in state courts.

This new law will not lead to abuse of people's privacy rights for several reasons. Judicial authorization for wiretaps will be very difficult to get and very expensive to conduct. The number of times this law will be used is very small. There has not been a history of abuse under the current federal or state law upon which the bill is based. The bill applies only to a very narrow and specific category of serious acts of terrorism. Law enforcement officers get very good training now, and can be trusted not to abuse authority they are given.

Terrorists are secretive and work in much the same way as some organized crime operations.
Existing federal law upon which this bill is based have worked well in fighting organized crime.

**Testimony Against:** Washington has historically been very protective of privacy rights and should continue to be so. This bill will allow too much invasion of privacy and may

be unconstitutional under the strict privacy rights provisions of the state constitution. The bill presents opportunities for the kinds of abuses that history has shown will occur when the government is given too much authority to conduct surveillance on citizens. The bill will result in many innocent people being caught in the web of terrorism investigations.

The bill is not needed and will not be effective. Everything in the bill and much more has been available to federal law enforcement authorities for years, yet none of it was able to stop the September 11 attack.

The expanded authority to intercept e-mail is particularly dangerous. Although the bill purports to limit such interceptions to non-content information such as address lines, there is no technology capable of doing that and the bill is likely to result in government officials obtaining the content of communications when they are not authorized to do so.

The bill allows trial by ambush by giving defendants inadequate advanced notice that interceptions have been done. Ten days before trial is not enough time. The bill does not require the government to notify people when requests to intercept their conversations have been denied.

**Testified:** (In support) Representative Hurst, prime sponsor; Tim Schellberg and Larry Erickson, Washington Association of Sheriffs and Police Chiefs; and Pat Sainsbury and Mike Lang, Washington Association of Prosecuting Attorneys.

(Opposed) Janet Sutherland, Radical Women; Kris Costello and Brian Phillips, Washington Association of Criminal Defense Lawyers; Jerry Sheehan, American Civil Liberties Union of Washington; and Marilynn Moch, Human Rights Commission.