STORAGE NAME: h1439.sec
DATE: February 18, 2002

HOUSE OF REPRESENTATIVES
COMMITTEE ON
SELECT COMMITTEE ON SECURITY
ANALYSIS

BILL #: HB 1439

RELATING TO: Interception of Communications

SPONSOR(S): Representative(s) Gelber

TIED BILL(S):

ORIGINATING COMMITTEE(S)/COUNCIL(S)/COMMITTEE(S) OF REFERENCE:

(1) SELECT COMMITTEE ON SECURITY
(2) JUDICIAL OVERSIGHT
(3) PROCEDURAL & REDISTRICTING COUNCIL
(4)
(5)

THIS DOCUMENT IS NOT INTENDED TO BE USED FOR THE PURPOSE OF CONSTRUING STATUTES, OR TO BE CONSTRUED AS AFFECTING, DEFINING, LIMITING, CONTROLLING, SPECIFYING, CLARIFYING, OR MODIFYING ANY LEGISLATION OR STATUTE.

I. SUMMARY:

Florida's laws governing the interception of communications are patterned after federal laws, and are found in chapter 934, F.S. In response to the terrorist activities of September 11, 2001, Congress passed the USA PATRIOT Act. Portions of that act effected changes in the federal wiretap laws to address advances in technology and new and emerging crimes, e.g., identity theft, terrorists' acts, etc. This bill amends several sections of chapter 934, F.S., conforming Florida's statutory language regarding interception of communications to recent changes in the federal law.

Pen Register and Trap and Trace Device: Sections of chapter 934, F.S., relating to pen registration and trap and trace devices are amended to apply to a broad variety of relatively new communications technologies, such as a cellular telephone number or an Internet user account or e-mail address. This bill clarifies that law enforcement may seek court authorization to use pen register and trap and trace devices to trace communications on the Internet and other computer networks. These devices may obtain information, including dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire and electronic communications, but cannot authorize the interception of the content of the communication. Florida state judges may issue orders authorizing the interception of wire communications with statewide effect provided there is some criminal activity nexus within the jurisdiction of the court initially authorizing the order. Additionally, this bill requires law enforcement officers to maintain and file a record with the court whenever they use a court order to install their own monitoring device on computers belonging to a public provider.

Computer Trespasser and Protected Computer: This bill defines computer trespasser and protected computer consistent with federal law. The bill will allow victims of computer attacks to authorize law enforcement officers to monitor trespassers on their computer systems. Here, law enforcement officers may intercept communications of a computer trespasser transmitted to, through, or from a protected computer under certain circumstances.

Miscellaneous Provisions: The bill has several other various provisions relating to interception of communications. Some include:

- Allowing court-ordered interception in criminal investigations of bombs and weapons of mass destruction;
- Empowering the Florida Department of Law Enforcement (FDLE) to utilize resources effectively to investigate acts of terrorism, including use of personnel from other agencies who would be acting at the direction of FDLE;
- Providing a method whereby FDLE is brought into local agency's wire interception investigations when those cases have uncovered evidence of terrorism-related crimes; and
- Allowing emergency intercepts when there is evidence that communications involve activities threatening national or state security.

II. SUBSTANTIVE ANALYSIS:

A. DOES THE BILL SUPPORT THE FOLLOWING PRINCIPLES:

1.	Less Government	Yes []	No [X]	N/A []
2.	Lower Taxes	Yes []	No []	N/A [X]
3.	Individual Freedom	Yes []	No []	N/A [X]
4.	Personal Responsibility	Yes []	No []	N/A [X]
5.	Family Empowerment	Yes []	No []	N/A [X]

For any principle that received a "no" above, please explain:

Less Government: New authority and requirements imposed upon law enforcement agencies and judges pertaining to the interception of communications do not support the principle of less government.

B. PRESENT SITUATION:

Florida's wiretap laws are patterned after federal law. With the enactment of the USA PATRIOT Act on October 26, 2001, the federal wiretap laws have been modernized to reflect recent changes in technology and needed changes for criminal investigations. Because of these changes, Florida's laws no longer conform to its federal counterpart.

Section 934.02, F.S., is the definitional section of chapter 934 pertaining to security of communications.

Section 934.03, F.S., establishes various prohibitions against the interception and disclosure of wire, oral, or electronic communications. Criminal punishments range from a second-degree misdemeanor to a third-degree felony. Conversely, this section addresses several scenarios wherein the interception of a communication is permitted.

Section 934.07, F.S., provides the Governor, the Attorney General, the Statewide Prosecutor, or any State Attorney may authorize an application to a judge of competent jurisdiction for an order authorizing the interception of wire, oral, or electronic communications by the Department of Law Enforcement (FDLE) or any law enforcement agency (as defined in § 934.02, F.S.) having responsibility for the investigation of the offense for which the application is made when such interception may provide or has provided evidence of the commission of certain offenses. The offenses include: murder; kidnapping; aircraft piracy; arson; gambling; robbery; burglary theft dealing in stolen property; criminal usury, bribery, or extortion; any violation of chapters 815 (computer-related crimes), 847 (obscenity), 893 (drug abuse prevention and control), 895 (Florida RICO Act), or 896 (offenses related to financial transactions); any violation of the provisions of the Florida Anti-Fencing Act; any violation of § 827.071 (sexual performance by a child) or § 944.40 (escapes); or any conspiracy or solicitation to commit any violation of the laws of this state relating to such offenses.

This section was amended by chapter 2001-350, Laws of Florida, which enacted legislation passed during Special Session C in December 2001. Those changes authorize a court to grant FDLE's application to intercept communications that evidence the commission of any offense that may be related to an act of terrorism. Chapter 2001-350, Laws of Florida, defines "terrorism" as an activity that:

- Involves a violent act or an act dangerous to human life that is a violation of the criminal laws of Florida or federal law; or
- Involves a violation of s. 815.06, F.S. (offenses against computer users); and
- Is intended to:
    - Intimidate, injure, or coerce a civilian population;
    - Influence the policy of a government by intimidation or coercion; or
    - Affect the conduct of government through destruction of property, assassination, murder, or kidnapping, or aircraft piracy.[1]

Section 934.09, F.S. Subsection (7) of § 934.09, F.S., establishes emergency intercept procedures for law enforcement agencies.[2] To qualify under the emergency intercept provisions of this section, the officer must reasonably determine that an emergency exists, i.e., circumstances involving immediate danger of death or serious injury or the escape of a prisoner requires the communication to be intercepted before an authorizing order can be obtained and there are grounds upon which a court could order such interception under chapter 934, F.S. Additionally, when a law enforcement agency acts under these emergency conditions, it must submit a written application for court approval within 48 hours of the emergency intercept.

Section 934.09(1), F.S., sets forth the procedures by which communications may be intercepted. This section requires that an application for a court order authorizing or approving the interception of a wire, oral, or electronic communication under §§ 934.03--934.09, F.S., must be made in writing upon oath or affirmation to a judge of competent jurisdiction and must state the applicant's authority to make such application. Among the information the statute specifies must be included in the application is a particular description of the nature and location of the facilities from which, or the place where, the communications are to be intercepted. Section 934.09(11), F.S., contains exemptions to this requirement.

Section 934.09(11), F.S., provides that the requirements of subparagraph (1)(b)2. and paragraph (3)(d) of that section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted <u>do not apply if</u>:

(b) In the case of an application with respect to a wire or electronic communication:

1. The application is by an agent or officer of a law enforcement agency and is approved by the Governor, the Attorney General, the statewide prosecutor, or a state attorney.

2. The application identifies the person believed to be committing the offense and whose communications are to be intercepted, and the applicant makes a showing there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility or that the person whose communications are to be intercepted has removed, or is likely to remove, himself or herself to another judicial circuit within the state.

3. The judge finds such showing has been adequately made.

4. The order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

---

[1] Section 934.07, F.S., was further amended by chapter 2001-350, Laws of Florida, by adding aircraft piracy and solicitation to the enumerated offenses whereby an application for a wiretap order may be sought.

[2] Florida's emergency intercept authorization under § 934.09(7), F.S., was enacted in 2000. *See* § 11, chapter 2000-369, Laws of Florida.

For terrorism investigations, § 934.09, F.S., specifically allows a court to authorize continued interception throughout Florida if the original interception occurred within the court's jurisdiction. This provision will sunset on July 1, 2004.

Section 934.08, F.S., establishes parameters whereby investigative or law enforcement officers may disclose the contents of certain intercepted communications to:

- The Department of Legal Affairs for investigations or proceedings involving deceptive and unfair trade practices and Florida's anti-trust and RICO laws;
- Any attorney authorized by law to investigate and institute actions on behalf of the state or a political subdivision of the state; or
- Another investigative or law enforcement officer if the disclosure is appropriate to the performance of the officer or person making or receiving the disclosure.

Section 934.22, F.S. provides that electronic communications service or remote computing service providers may not disclose the contents of a communication while they have it in electronic storage or it is carried or maintained by the service. This section provides for several exceptions to the no-disclosure rule. Some of those exceptions, which allow disclosure, include:

- With lawful consent of the originator or an addressee or intended recipient of the communication or the subscriber, in the case of a remote computer service; and
- To a law enforcement agency if the contents of the communication was inadvertently obtained and appear to pertain to the commission of a crime.

Section 934.23, F.S., sets forth the requirements law enforcement officers must meet in order to compel a provider of an electronic communication service or a remote computing service to disclose certain information pertaining to electronic communications and customer records. This section authorizes law enforcement officers to obtain a warrant, subpoena, or court order for such disclosure.

Section 934.27, F.S., establishes a civil cause of action for one seeking relief and/or damages where there is a knowing or intentional violation of the procedures set forth in §§ 934.21—934.28, F.S., (unlawful access to stored communications; unlawful use of a two-way communications device; disclosure of contents; requirements for governmental access; back-up copies of communications and customer notification). This section sets a 2-year statute of limitations on these actions and defines what relief may be sought.

The section sets forth a complete defense to any civil or criminal action where one, in good faith, relies upon:

- A warrant or court order, subpoena, or a statutory authorization;
- A law enforcement officer request under § 934.09(7), F.S.; and
- A determination that § 934.03(3), F.S., permitted the conduct complained of.

Section 934.31, F.S. provides general prohibitions on the use of information obtained using a pen register or a trap and trace device. The information obtain by these devices must be limited to the recording or decoding of electronic impulses to the dialing and signaling information used in processing calls.

Section 934.33, F.S., establishes the procedures for issuance of a pen register or a trap and trace device order. An application, conforming to the requirements of § 934.32, F.S., must be submitted to a court and the applicant must certify to the court that the information sought is relevant to an ongoing criminal investigation. This section sets forth the information the court must include in its order, which is sealed until otherwise ordered by the court. The authorization to install and use a pen register or a trap and trace device is limited to no more than 60 days.

Section 934.34, F.S., provides that wire or electronic communications service providers must, upon the request of the applicant, provide facilities and technical assistance in assisting the applicant in installing a pen register or a trap and trace device. Providers are allowed reasonable compensation for their expenses incurred in providing such facilities and assistance.

C. EFFECT OF PROPOSED CHANGES:

Section 934.02, F.S., is amended by revising or adding the following definitions:

- "Wire communication" is amended to delete the electronic storage of communications from the definition.
- "Judge of competent jurisdiction" is revised to clarify that the geographic location of the judge is not a component of the definition. This change will permit any state judge having felony jurisdiction to authorize initial and ongoing interception of communications anywhere in the state when there is a nexus between the investigation and the offense to the jurisdiction in which the judge presides.
- "Electronic communications system" is amended to add wire communications to the definition.
- "Pen register" is expanded to include a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted from the instrument or facility from which the communication is transmitted. The amended definition specifically excludes the content of any intercepted communication.
- "Trap and trace device" is also expanded to capture incoming electronic or other impulses that identify dialing, routing, addressing, or signaling information reasonably likely to identify the source of the communication. Such information does not include the content of the communication.
- "Foreign intelligence information" is new to chapter 943, and is patterned after a similar definition that was added to § 2510 of Title 18, United States Code in the USA PATRIOT Act. This term is used in new language added in section 6 of the bill that amends § 934.08, F.S., authorizing disclosure and use of certain intercepted communications.
- "Protected computer" and "computer trespasser" are new definitions that track the changes in federal law. These definitions are added to permit law enforcement officers, at the request of the computer owner, to monitor computer trespassers.

Section 934.03, F.S., is amended to track federal changes in the USA PATRIOT Act. This will allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. The bill allows officers to intercept communications of a computer trespasser transmitted to, through, or from a "protected computer" if:

- Authorized by the owner/operator of the protected computer;
- The officer is lawfully engaged in an investigation;
- The officer has reasonable grounds to believe the communications will be relevant to the investigation; and
- The interception only acquires communications to, through, or from the computer trespasser.

This change allows victims of computer trespass to permit experts to lawfully access their computers in an attempt to stop the criminal conduct and identify the perpetrators.

Section 934.07, F.S., is amended to permit law enforcement officers to request court-ordered interception of communications in investigations involving destructive devices (§§ 790.161, 790.1615, and 790.162, F.S.), false bomb reports (§§ 790.163 and 790.164, F.S.), hoax bombs (§ 790.165, F.S.), and weapons of mass destruction and hoax weapons of mass destruction (§ 790.166, F.S.) criminal offenses.

Subsection (1)(b) of § 934.07, F.S., is amended to permit FDLE to utilize outside resources to assist in the investigation of terrorists acts, including use of personnel from other agencies.

To promote interdepartmental communications, this section is also amended to establish a method by which FDLE is brought into a local agency's communication interception investigation if that investigation has turned to terrorism-related crimes. Specifically, a local agency is required to notify FDLE if terrorism information is obtained pursuant to an existing wiretap in an investigation. FDLE, upon such notification, must promptly review the information and determine whether the information relates to an actual or anticipated act of terrorism. The bill also authorizes FDLE to apply for a court order authorizing it to investigate this information relating to terrorism if probable cause exists that the contents of the intercepted communications are evidence of acts of terrorism. Alternately, FDLE may request the local law enforcement agency to join it in seeking a modification of the original interception order. The bill provides the emergency provisions of § 934.09(7), F.S., are applicable to FDLE under these circumstances of receiving terrorist intelligence from local law enforcement agencies.

Section 934.09, F.S. Subsection (7) is amended to add an option for an emergency intercept that is consistent with federal law, specifically allowing emergency interceptions of communications when there is evidence the communications involve conspiratorial activities threatening national or state security.

The bill amends § 934.09(11), F.S., to clarify a judge may enter an order for interception of communications anywhere throughout the State of Florida when the application indicates a criminal or investigative nexus to a qualifying offense in the court's jurisdictional boundaries.

This bill removes the July 1, 2004, sunset provision in § 934.09(11), F.S., as amended by chapter 2001-359, Laws of Florida.

Section 934.08, F.S. Section 934.08(1), F.S., is amended by adding paragraph (b) to authorize an investigative or law enforcement officer, who, by authorized means, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, to disclose such contents to other enumerated officials to the extent that such contents include foreign intelligence or counterintelligence. This information may be shared with any state or federal law enforcement official, protective services official, defense official, security official, or federal immigration official. This new language is patterned after similar language enacted in the USA PATRIOT Act in 2001.

Section 934.22, F.S. The bill makes a several technical changes to conform with the changes made to the federal law in the USA PATRIOT Act. The changes are designed to enhance public safety during emergency situations.

Subsection (1) is amended to prohibit a provider of electronic communication service or a provider of remote computing service from disclosing to any governmental entity records or other information pertaining to a subscriber or customer. The current law enforcement exception to this rule is expanded to authorize a provider to voluntarily reveal information to law enforcement if the provider reasonably believes an emergency involving immediate danger of death or serious injury requires immediate disclosure of the information.

Additionally, a provider may disclose a record or other information of a subscriber or customer:

- If such disclosure is authorized under § 934.23, F.S., pertaining to requirements for government access;
- If the provider has the consent of the customer or subscriber;
- If such disclosure is incident to rendering service or protecting the rights or property of the provider of the service;
- To a governmental entity if the provider reasonably believes an emergency involving immediate danger of death or serious injury requires immediate disclosure of the information; or

- To any person other than a governmental entity.

The bill specifically precludes disclosure of information protected under § 934.22(1)(a) and (1)(b), F.S.

Section 934.23, F.S. The bill makes several technical changes to this section, conforming it to recent changes in federal law. The changes establish parameters for required disclosure of customer communications or records maintained by remote computing services and electronic communication services to governmental entities. The bill provides greater specificity concerning the types of information that must be released pursuant to subpoena, court order, warrant, or owner consent.

The list of required disclosure of customer communications or records is expanded to include wire communications held by electronic communication service or remote computing service providers. Similarly, the list of authorized information that can be disclosed by these providers is expanded to include: local and long distance telephone connection records; records of session times or durations; length of service; type of service used; telephone or instrument number or other subscriber number or identity; and means and source of payment.

Section 934.27, F.S., is amended by extending relief from civil liability to cases in which a law enforcement officer requests that records be preserved in accordance with current law. This provision extends protections to the providers of services that include individual citizens and companies.

Section 934.31, F.S. Subsection (3) currently requires law enforcement officers using a pen register to use technology that restricts the recording or decoding of electronic impulses to the dialing and signaling information used to process the call. The bill amends this provision to apply the restrictions of this section to trap and trace devices. The bill also clarifies that the contents of any wire or electronic communications subject to a pen register or trap and trace device are not recorded or decoded. This bill also extends emergency use when there is evidence the intercepted communications involve conspiratorial activities threatening national or state security.

Section 934.33 F.S. The changes to this section are designed to protect telecommunication businesses and Internet service providers. These changes are also patterned after changes to federal law made through the enactment of the USA PATRIOT Act.

Specifically, an officer serving an order for a pen register or a trap and trace device, if requested by a person or entity, must provide the company with written or electronic certification that the order applies to the person or entity being served if they are not specifically named in the order. This gives the person or entity the right to demand certification that the order applies to them, thus triggering their ability to claim protection from civil and criminal liability under § 934.27, F.S., due to their good-faith execution of a lawful order.

The bill also requires law enforcement agencies using their own pen register or trap and trace devices pursuant to a court order must ensure a record is maintained that identifies:

- The officer(s) who installed the device and who accessed the device to obtain information;
- The date and time the device was installed and uninstalled, as well as the duration of each occasion the device was used;
- Configuration of the device at the time of installation and any subsequent modifications; and
- Information collected by the device.

This record must be provided *ex parte* and under seal to the court that issued the original order authorizing the installation within 30 days after termination of the order, including any extensions of the order.

Section 934.34, F.S., is amended to conform to federal law and other changes made in the bill. It addresses changes in technology regarding where and how trap and trace devices may be installed. Specifically, the bill requires the provider of a wire or electronic communication to, at the request of an authorized applicant, install a trap and trace device on the appropriate line "or other facility."

D. SECTION-BY-SECTION ANALYSIS:

Please refer to Present Situation and Effect of Proposed Changes sections for a description of the bill.

III. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT:

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

Indeterminate.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

Indeterminate.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

IV. CONSEQUENCES OF ARTICLE VII, SECTION 18 OF THE FLORIDA CONSTITUTION:

A. APPLICABILITY OF THE MANDATES PROVISION:

This bill does not require cities or counties to spend funds or to take actions requiring expenditure.

B. REDUCTION OF REVENUE RAISING AUTHORITY:

This bill does not reduce the authority that municipalities or counties have to raise revenues in the aggregate.

C. REDUCTION OF STATE TAX SHARED WITH COUNTIES AND MUNICIPALITIES:

This bill does not reduce the percentage of a state tax shared with counties or municipalities.

V. COMMENTS:

A. CONSTITUTIONAL ISSUES:

None.

B. RULE-MAKING AUTHORITY:

None.

C. OTHER COMMENTS:

None.

VI. AMENDMENTS OR COMMITTEE SUBSTITUTE CHANGES:

None.

VII. SIGNATURES:

COMMITTEE ON SELECT COMMITTEE ON SECURITY:

Prepared by:	Staff Director:
Randy L. Havlicak	Thomas J. Randle / Richard Hixson