SENATE STAFF ANALYSIS AND ECONOMIC IMPACT STATEMENT

(This document is based only on the provisions contained in the legislation as of the latest date listed below.)

BILL: SB 1924

SPONSOR: Senator Brown-Waite

SUBJECT: Security of Communications

DATE: March 23, 2000 REVISED: _____ _____ _____ _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Erickson	Cannon	CJ	Favorable
2.			JU	
3.				
4.				
5.				

I. Summary:

Senate Bill 1924 revises ch. 934, F.S., Florida's Security of Communications Act, to bring Florida's laws relating to the security of wire, oral, and electronic communications into harmony with similar federal provisions (18 U.S.C. 2510, et. seq.). The bill has the practical effect of expanding law enforcement's authority to intercept communications, primarily by the authorization to intercept communications in certain emergency situations without first obtaining a court order. The main features of the bill are described below.

- A communications interception is authorized *without prior court approval but rather by applying for court approval of the interception within 48 hours after the interception is initiated* if an investigator or law enforcement officer reasonably determines that:
  - an emergency exists which involves immediate danger of death or serious physical injury to any person or the danger of escape of a prisoner; and
  - Requires that a communication be intercepted before an order authorizing such interception can, with due diligence, be obtained; and
  - there are grounds upon which an order could be entered under ch. 934, F.S., authorizing such interception.

  Escape of a prisoner is not specified as a basis for an emergency intercept under federal law, and therefore, would be unique to Florida law.

- An investigator or law enforcement officer is authorized to install and use emergency pen registers and emergency trap and trace devices in certain circumstances and subject to prescribed procedures.

- A third degree felony offense is created for intentional disclosure to an unauthorized party of the contents of a legally authorized communications interception.

- Prostitution is deleted from the list of prescribed offenses for which a communications interception may be authorized.

- Good faith reliance on a request from a law enforcement officer under the new emergency intercept provision is a complete defense to civil and criminal liability.

- The federal one-party consent law does not apply to construction of a defense based upon good faith reliance on Florida and federal law.

- Service providers and others are required to disclose certain information when law enforcement officers obtain a subpoena, such as the name, address, and telephone number of a subscriber or customer. The person seeking the intercept must compensate the service provider for reasonable expenses incurred in disclosing such information. The provider is immunized from civil and criminal liability for such disclosure.

- Service providers and others are required to assist an officer authorized by court order to install and use a pen register or trap and trace device, or authorized by law to install and use an emergency pen register or emergency trap and trace device. The person seeking the emergency intercept must compensate the service provider for reasonable expenses incurred in providing technical assistance relating to installation and use of an emergency pen register and trap and trace devices. The provider is immunized from civil and criminal liability for providing such assistance.

This bill substantially amends or creates the following sections of the Florida Statutes: 934.02; 934.03; 934.07; 934.09; 934.10; 934.23; 934.27; and 934.35.

II. Present Situation:

The last substantial amendments to ch. 934, F.S., Florida Security of Communications Act, occurred in 1989. Since that time, the federal law, upon which ch. 934, F.S., has been patterned, has been revised at least four times: 1994; 1996; 1997; and 1998. The similarities and differences between federal and Florida law are described below.

Definition of "Wire Communication"

Federal law defines a "wire communication" as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication." 18 U.S.C. 2510(1).

The federal law (18 U.S.C. 2510(1)) does not exempt cordless telephones, whereas current state law (s. 934.02(1), F.S.), does exempt cordless telephones.

Definition of "Electronic, Mechanical, or Other Device"

In the federal definition of "electronic, mechanical, or other device," reference is made to "a provider of wire or electronic communication service." 18 U.S.C. 2510(5)(a)ii. In Florida law, a similar definition refers to this provider as a "common communications carrier." s. 934.02(4), F.S.

Definition of "Electronic Communication"

The federal definition of "electronic communication" exempts electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage or transfer of funds. 18 U.S.C. 2510(12). The definition of "electronic communication" in Florida law does not contain a similar exemption. s. 934.02(12), F.S.

Prohibition Against Disclosure of Intercepted Communications

Federal law prohibits a person from intentionally disclosing, or endeavoring to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means provided for in various federal provisions. The person must:

- know or have reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation;
- have obtained or received the information in connection with a criminal investigation; and
- disclose or endeavor to disclose the information with the intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

The person who commits this prohibited act is subject to a fine or imprisonment of up to five years, or both, or to a suit by the federal government. 18 U.S.C. 2511(1)(e), (4), and (5). There is no similar provision in Florida law.

Federal law provides that it shall not be unlawful for an operator of a switchboard, or an officer, employee, or agent of a provider of a wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks. 18 U.S.C. 2511(2)(a)(I). Florida law contains a similar provision but only references the service provider's facilities which are used in transmission of wire communications. s. 934.03(2)(a)1., F.S.

Penalties for Unlawful Interception and Disclosure of Intercepted Communications

Federal law contains certain penalty provisions relating to unlawful interception and disclosure of wire, oral, or electronic communications that only apply if:

- the offense is a first offense that is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; and

- if the wire or electronic communication is not scrambled, encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication.

Subject to the conditions described, the offense committed is punishable by a fine or imprisonment of not more than five years, or both, if the communication is not (or only a fine if the communication is):

- the radio portion of a cellular telephone communication;

- a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit; or

- a public land mobile radio service communication or a page service; and communication. 18 U.S.C. 2511(4)(b)(I) and (ii).

Florida law contains misdemeanor penalty provisions similar to the described federal penalty provisions but does not refer to cordless telephone communication. s. 934.03(4)(b)1. and 2., F.S.

Procedures for Interception of Communications; Obtaining Court Authorization

18 U.S.C. 2518 contains the federal procedures for interception of wire, oral, or electronic communication. An application for an order authorizing an interception must include a number of different pieces of information, including a particular description of the nature and location of the facilities from which, or the place where, the communication is to be intercepted. 18 U.S.C. (1)(b)(ii).

Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving the interception within the territorial jurisdiction of the court, if the judge determines on the basis of the facts submitted that certain specified conditions are met, including that there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of various offenses as described under 18 U.S.C. 2516, or are leased to, listed in the name of, or commonly used by such person.

Among the exemptions from these two requirements in 18 U.S.C. 2518 is an application with respect to a wire or electronic communication if:

- the application is by a federal investigative or law enforcement officer and is approved by the U.S. Attorney General or other designated officials;

- the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing *that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility*;

- the judge finds that such showing has been adequately made; *and*

- *the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.* 18 U.S.C. 2518(11)(b), as amended by Section 602, P.L. 105-272, 112 STAT. 2413 (italicized language indicating the amendments). Technical conforming changes were also made to 18 U.S.C. 2518(12). Id.

Florida law contains similar provisions patterned after 18 U.S.C. 2518(11)(b) and (12). s. 934.09(10)(b) and (11), F.S. However, the language in s. 934.09(10)(b) and (11), F.S., does not track the most recent amendments to 18 U.S.C. 2518(11)(b) and (12) made by Section 602, P.L. 105-272.

Emergency Interception of Communications; Interception of Communications Initiated Without Prior Court Authorization

Federal law contains an "emergency intercept" provision. This provision authorizes the U.S. Attorney General and other designated officials and officers to intercept communications *without prior court approval but rather by applying for court approval of the interception within 48 hours after the interception is initiated* if such officials or officers reasonably determine that:

- an emergency exists which involves immediate danger of death or serious physical injury, conspiratorial activities threatening the national security, or conspiratorial activities characteristic of organized crime which requires that a communication be intercepted before an order authorizing such interception can, with due diligence, be obtained; and

- there are grounds upon which an order could be entered authorizing such interception. 18 U.S.C. 2518(7).

In the absence of an order, such interception must immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application is denied, or in any other case in which the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted must be treated as having been obtained in violation of federal law, and an inventory must be served on the person named in the application. Id.

There is no similar "emergency intercept" provision in Florida law.

Communications Interception and Prostitution-Related Offenses

Section 934.07, F.S., authorizes the interception of wire, oral, or electronic communications by law enforcement when the interception may provide evidence of a list of enumerated offenses. Prostitution is listed among those enumerated offenses. In *State v. Rivers*, 660 So.2d 1360 (Fla. 1995), the Florida Supreme Court held that, because the federal wiretap statute did not authorize wiretaps to investigate nonviolent prostitution-related offenses, the federal law preempted the authority under s. 934.07, F.S., to permit such wiretaps.

Assistance From Communications Service Providers

Relevant to the federal emergency intercept provision, a provider of a wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized under federal law to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, if such provider or other specified person has been provided with a written certification from the U.S. Attorney General or other persons authorized to conduct emergency intercepts states that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required. The certification must also set forth the time period during which the provision of information, facilities, or technical assistance is authorized and specify the information, facilities, or technical assistance required. 18 U.S.C. 2511(2)(a)(ii)(B).

Civil and Criminal Immunity

While federal law provides for a civil cause of action against a person or entity engaged in an unlawful intercept, disclosure, or intentional use of wire, oral, or electronic communication, a good faith reliance by such person or entity on a request by an investigative or law enforcement officer under the emergency intercept provision is a complete defense against any civil or criminal action brought under federal law. 18 U.S.C. 2520(d)(2).

Florida law contains a provision similar to federal law. s. 934.10, F.S.

In *Wood v. State*, 654 So.2d 218 (Fla. 1st DCA 1995), the First District Court of Appeals held that the trial court abused its discretion by forbidding the defendant from presenting evidence that he illegally taped his ex-wife's telephone conversations out of a good faith belief that to do so was not illegal. The Court also held that the trial court erred in denying the defendant's proffer of testimony relevant to this defense and refusing to instruct the jury on this defense.

The defendant in this case relied on 18 U.S.C. 2511(2)(d) which provides that it is not unlawful for a person not acting under color of law to intercept a communication where such person is a party to the communication or where *one* of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the federal Constitution or federal or state laws. Unlike 18 U.S.C. 2511(2)(d), s. 934.03, F.S., requires that all parties to a communication consent to the interception.

The Court noted that the plain language of s. 934.10, F.S., simply states that a good faith reliance on a good faith determination that *federal* or Florida law permits the conduct complained of shall

constitute a complete defense to any criminal action arising out of the conduct. Given the particular facts of the case, such as the fact that the defendant was serving as his own legal researcher and, for a certain time, as his own counsel, and the fact that the attorney whom he eventually obtained agreed with the defendant's interpretation of s. 934.10, F.S., as permitting a one-party intercept, defendant's proffered testimony relating to such facts was relevant to this defense and reasonably related to the issues at trial.

Authorization to Install and Use a Pen Register or Trap and Trace Device

A "pen register" is an electronic device that records or decodes electronic or other impulses that identify the numbers dialed or otherwise transmitted on the telephone line to which this device is attached. This device also records the time, date, and duration of an outgoing phone call, and the time of day that incoming ringing signals were received but not the number of the telephone from which the incoming phone call is made.

The term "pen register" is a somewhat archaic term that has survived the transition from pulse dialing to touch-tone dialing. The recording device is now often referred to as a "Dial Number Recorder" or "DNR."

A pen register might be used, for example, on a suspected drug dealer's phone line to provide investigators with leads as to the dealer's suppliers and customers.

A "trap and trace device" or "phone trap" is a device that compiles a record of the telephone numbers of the phones from which calls to a certain phone were made. "Caller ID" is a version of the "trap and trace device." Use of this device is lawful because it is installed by, or at the request of, the subscriber.

A trap and trace device might be used, for example, in a situation in which investigators expect that an extortionist or kidnapper will make a demand over a particular phone.

By using a pen register and a trap and trace device, investigators can obtain an on-going record of all calls to and from a particular phone.

Federal law provides that a government agency authorized to install and use a pen register under federal or state law must use technology reasonably available to the agency that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing. 18 U.S.C. 3121(c).

Pursuant to a request from an attorney for the federal government or an officer of a law enforcement agency authorized by federal law to receive the results of a trap and trace device, a provider of a wire or electronic communication service, landlord, custodian, or other person, must install such device on the appropriate line and furnish to the investigative or law enforcement officer all additional information, facilities, and technical assistance including installation and operation of the device. 18 U.S.C. 3124(b).

While 18 U.S.C. 2518 authorizes an emergency intercept, 18 U.S.C. 3125 specifically provides authorization for the installation and use of a pen register or a trap and trace device. The procedures are essentially the same as contained in 18 U.S.C. 2518.

Access to Stored Electronic Records

Federal law prescribes requirements for governmental access to stored electronic records. A provider of an electronic communication service or remote computing service must disclose a record or other information pertaining to a subscriber to, or customer of, such service (with some exclusions) to a governmental entity only when the governmental entity:

- obtains a warrant issued under the Federal Rules of Criminal Procedure or an equivalent state warrant;

- obtains a court order for such disclosure if:

    - the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation; and

    - in the case of a state governmental authority, such a court order is not prohibited by the law of such state;

- has the consent of the subscriber or customer to such disclosure; or

- submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider who are engaged in telemarketing. 18 U.S.C. 2703(c)(1)(B).

Florida law does not contain a provision similar to the communications disclosure provision described above.

Disclosure by Communications Service Providers

When the governmental entity uses an administrative subpoena authorized by a federal or state statute, federal or state grand jury, a trial subpoena, or any means described above for the purpose of obtaining records or other information pertaining to a customer or subscriber of an electronic communication service or remote computing service, the provider of such service must disclose to the governmental entity the following information:

- name;
- address;
- local and long distance telephone toll billing record;
- telephone number or other subscriber number or identity; and
- length of services and types of services utilized. 18 U.S.C. 2713(c)(1)(C).

Federal law requires a provider of a wire or electronic communication service, upon the request of a governmental entity, to take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process for a period of 90 days, subject to an additional 90-day extension upon a renewed request by the governmental entity. 18 U.S.C. 2703(f)(1) and (2).

Florida law does not contain a provision similar to the records disclosure provision described above.

III. Effect of Proposed Changes:

Senate Bill 1924 revises ch. 934, F.S., Florida's Security of Communications Act, to bring Florida's laws relating to the security of wire, oral, and electronic communications into harmony with similar federal provisions (18 U.S.C. 2510, et. seq.). The bill has the practical effect of expanding law enforcement's authority to intercept communications, primarily by the authorization to intercept communications in certain emergency situations without first obtaining a court order.

Provided is a section-by-section analysis of SB 1924.

Section 1

- The definition of "wire communication" in s. 934.02, F.S., is amended to remove an exemption from ch. 934, F.S., that previously existed for cordless telephones, to parallel the federal definition in 18 U.S.C. 2510(1).

- The phrase "provider of wire or electronic communication service" in s. 934.02, F.S., is substituted for "communications common carrier" in the definition of "electronic, mechanical, or other device" to parallel the federal definition in 18 U.S.C. 2510(5)(a)(ii).

- The definition of "electronic communication" in s. 934.02, F.S., is amended to add an exemption for electronic funds transfer information stored by a financial institution to parallel the federal definition of "electronic communication" and identical exemption in 18 U.S.C. 2510(12). This type of information is covered under other provisions relating to stored electronic communications.

Section 2

- A new third degree felony offense is created in s. 934.03, F.S. The provision prohibits intentional disclosure of the contents of a legally authorized communications interception to an unauthorized party, consistent with a similar criminal offense provision in 18 U.S.C. 2511(1)(e).

- Misdemeanor penalty provisions in s. 934.03, F.S., relating to unlawful interception or disclosure of communications are amended to include reference to cordless telephones for the purpose of application of those penalty provisions. These changes are consistent with similar penalty provisions in 18 U.S.C. 2511(4)(b), (4)(b)(I), and (4)(b)(ii).

- "Electronic communications" is added to a provision in s. 934.03, F.S., allowing service providers to intercept communications while engaged in any activity which is a necessary incident to the rendition of the provider's service or to the protection of the rights or property of the service provider, consistent with a similar provision in 18 U.S.C. 2511(2)(a)(I).

- Section 934.03, F.S., is amended to provide that a provider of a wire, oral, or electronic communication service and other designated persons may provide information, facilities, or technical assistance to a person authorized by law to intercept such communications if the provider or other designated person has been provided with a certification in writing by a person authorized to conduct an emergency intercept stating that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required. This provision is similar to the federal provision in 18 U.S.C. 2511(2)(a)(ii)(B).

Section 3

- Section 934.07, F.S., is amended to delete prostitution from the list of enumerated offenses for which a communications interception is authorized, consistent with *State v. Rivers*, 660 So.2d 1360 (Fla. 1995), in which the Florida Supreme Court held that, because the federal wiretap statute did not authorize wiretaps to investigate nonviolent prostitution-related offenses, the federal law preempted the authority under s. 934.07, F.S., to permit such wiretaps.

Section 4

- Section 934.09, F.S., is amended to add a new "emergency intercept" provision which authorizes a communications interception *without prior court approval but rather by applying for court approval of the interception within 48 hours after the interception is initiated* if an investigator or law enforcement officer reasonably determines that:

  - an emergency exists which involves immediate danger of death or serious physical injury to any person or escape of a prisoner; and

  - requires that a wire, oral, or electronic communication be intercepted before an order authorizing such interception can, with due diligence, be obtained; and

  - there are grounds upon which an order could be entered under ch. 934, F.S., authorizing such interception.

  This emergency intercept provision and the procedures prescribed for an emergency intercept are similar to the federal provision in 18 U.S.C. 2518(7) with two exceptions. First, the bill does not include, like the federal law, "conspiratorial activities threatening the national security" or "conspiratorial activities characteristic of organized crime" as a basis for an emergency intercept. Second, the bill includes escape of a prisoner as a basis for an emergency intercept, which is not included in federal law.

- Exemptions from particular procedures for an interception order, which are patterned on similar exemptions in 18 U.S.C. 2518 are amended to track the most recent changes to 18 U.S.C. 2518 made by Section 602, P.L. 105-272.

Section 5

- Section 934.10, F.S., is amended to provide that a good faith reliance on a request of an investigative or law enforcement officer under the new emergency intercept provision is a complete defense to any civil or criminal action, or administrative action, arising out of various statutory provisions relating to the interception, disclosure, or use of a wire, oral, or electronic communication. This provision is similar to the federal provision in 18 U.S.C. 2520(d)(2).

- The bill also provides that the federal one-party consent law does not apply to construction of a defense in s. 934.10, F.S., based upon good faith reliance on Florida and federal law. The effect of this change is that Florida's law which requires consent of all parties to a communications interception is relevant to this defense, not the federal provision which only requires the consent of one party.

Section 6

- Section 934.23, F.S., is amended to specify the types of information a service provider must disclose when investigative or law enforcement officers obtain a subpoena, such as the name, address, telephone toll billing records, telephone number, and length of service as a subscriber to, or customer of, such service, and the types of services the subscriber or customer used. This new provision and additional new provisions relating to the preservation of records for a specified time period are similar to the federal provisions in 18 U.S.C. 2703(c)(1)(B) and (C), (c)(2), (d), and (f)(1) and (2).

- The person seeking the intercept must compensate the service provider for reasonable expenses incurred in disclosing such information. The provider is immunized from civil and criminal liability for such disclosure.

Section 7

- Section 934.10, F.S., is amended to provide that a good faith reliance on a request of an investigative or law enforcement officer under the new emergency intercept provision is a complete defense to any civil or criminal action arising out of various statutory provisions relating to access to, and disclosure of, stored communications. This provision is similar to the federal provision in 18 U.S.C. 2707(e)(2) and (3).

Section 8

- Section 943.31, F.S., is amended to provide that an investigative or law enforcement officer authorized to install and use a pen register must use technology reasonably available to him or her. This provision is similar to the federal provision in 18 U.S.C. 3121(c).

Section 9

- Section 934.34, F.S., is amended to specify the duty of a service provider and other designated persons to assist those officials or officers authorized by court order to install and use a pen register or trap and trace device or conduct an emergency pen register or trap and trace installation. The provisions are similar to federal provisions in 18 U.S.C. 3124(b).

Section 10

- Section 934.35, F.S., is created. In substance, it is similar to the new emergency intercept provisions in s. 943.09, F.S., but is specific to emergency pen registers and trap and trace devices.

  The new section also requires that a service provider and others who furnish facilities or technical assistance be reasonably compensated for reasonable expenses incurred in providing such facilities and assistance. Further, the provider is immunized from civil and criminal liability for providing such assistance.

  The provisions are similar to the federal provisions in 18 U.S.C. 3125.

Section 11

- The effective date of the bill is October 1, 2000.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Economic Impact and Fiscal Note:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

None.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Amendments:

None.