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: CS/SB 1924

SPONSOR: Judiciary Committee and Senator Brown-Waite

SUBJECT: Security of Communications

DATE: April 13, 2000 REVISED: _____ _____ _____ _____

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

I. Summary:

This bill revises the Florida Security of Communications Act in chapter 934, F.S., relating to wiretapping of wire, oral, and electronic communications, to conform in part with its federal counterpart (18 U.S.C. 2510, et. seq.). The bill has the cumulative effect of expanding law enforcement's authority to intercept communications as follows:

- Subjects previously exempted cordless telephones and communications thereunder and electronic funds transfer information stored by a financial institution to the wiretap provisions;
- Authorizes an "emergency intercept" of communications and emergency installation and use of pen registers and trap and trace devices without prior court approval under specified circumstances and subject to prescribed procedures;
- Expands law civil and criminal immunity for law enforcement who act in good faith reliance under the emergency wiretap provisions;
- Creates a third degree felony offense for the intentional disclosure to an unauthorized party of the contents of a legally authorized communications interception;
- Removes the offense of prostitution from the list of prescribed offenses for which a communications interception may be authorized;
- Requires service providers and others to disclose specific information pursuant to a subpoena request subject to compensation and provides these providers with civil and criminal liability for such disclosure; and
- Requires service providers and others to assist in the installation and use of a pen register or trap and trace device subject to compensation, and provides these providers with civil and criminal immunity for assistance with such installation,

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 Florida Security of Communications Act in chapter 934, F.S., is patterned on a similar federal law. Although Florida's law has not been substantively amended since 1989, its federal counterpart has been amended at least four times with the most recent amendments in 1998. *See* P.L. 105-272, s. 604. Both the federal and Florida laws define the circumstances and conditions under which the interception of wire, oral and electronic communications are prohibited and authorized. Some of the major similarities and differences[1] between the federal and Florida law are described below.

- **Definitions**

Wire communication: Under federal law, the term *wire communication* is defined 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." *See* 18 U.S.C. 2510(1). Under Florida law, the term is identically defined except that it excludes the radio portion of the cordless telephone from the definition for *wire communication*. *See* s. 934.02(1), F.S.

Electronic, Mechanical, or Other Device: Under federal law, the term "electronic, mechanical, or other device," includes a reference to "a provider of wire or electronic communication service." 18 U.S.C. 2510(5)(a)ii. Under Florida law, the term used to refer to this provider is "common communications carrier." *See* s. 934.02(4), F.S.

Electronic Communication: Under federal law, the term "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. *See* 18 U.S.C. 2510(12). Under Florida law, the term does not exempt electronic funds transfer from the provisions of this chapter. *See* s. 934.02(12), F.S.

- **Prohibition Against Disclosure of Intercepted Communications**

Under federal law, a person may not intentionally disclose or endeavor to disclose to any unauthorized person the contents of a legally intercepted wire, oral or electronic communication. In order to be criminally or civilly liable for this offense, it must be shown that the person: 1)

[1]For example, unlike state law, federal law: 1) Requires annual reporting to the legislature regarding the number of applications and orders for pen registers and trap and trace devices (18 U.S.C. 3126), 2) Provides specific injunction relief against illegal interception of communications (18 U.S.C. 2521), 3) Requires monthly judicial reports of intercepted wire, oral or electronic communications to the U.S. Courts' Administrative Office (18 U.S.C. 2519(1)), 4) Requires annual reports from the Attorney General or statewide prosecutor regarding intercepted wire, oral or electronic communications (18 U.S.C. 2519(2)), 5) Requires annual reports of such intercepted communications from the Administrative Office of the United States Courts to Congress (18 U.S.C. 2519(3)), and 6) Provides a narrower category of persons who may apply for authorization for interception of communications or installation of pen registers or trap and trace devices.

Knew or had reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation; 2) Obtained or received the information in connection with a criminal investigation; and 3) Disclosed or endeavored to disclose the information with the intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation. The offense is punishable by up to 5 years in prison or by a fine, or both, and may additionally subject the person to a suit by the federal government. *See* 18 U.S.C. 2511(1)(e), (4), and (5). Under Florida law, there is no similar provision.

In contrast, under federal law, 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, may intercept, disclose, or use that communication in the normal course of his or her employment while engaged in any activity which is necessarily incidental to the rendition of service or to the protection of that service provider's rights or property. However, a wire communication service provider may not use service observing or random monitoring except for conducting mechanical or service quality control checks. *See* 18 U.S.C. 2511(2)(a)(I). Under Florida law, there is a similar provision but it is limited to those facilities which are used in the transmission of wire communications. *See* 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

Under federal law, the procedures for authorized interception of wire, oral, or electronic communications are set forth in 18 U.S.C. 2518. An application for an order authorizing an interception must include specified 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). The court may enter an ex parte order. The order may authorize or approve the interception within the territorial jurisdiction of the court. The order must be based on a determination that certain specified conditions have been met based on the facts submitted, 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.

There are exemptions from these procedural requirements 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. Under Florida law, similarly to federal law, no evidence obtained from intercepted wire or oral communications can be used in hearings, trials or proceedings before specified governmental bodies if the disclosure of that information would be in violation of the chapter.

Emergency Interception of Communications Without Prior Court Authorization
Under federal law, the U.S. Attorney General and other specially designated officials and officers may conduct an emergency interception of a communications without prior court approval but must secure the approval within 48 hours after an interception is initiated, provided that 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. The contents of such interception must be treated as having been obtained in violation of federal law if the application is denied or the interception is otherwise terminated without an order having been issued. An inventory of such intercepted communication must then be served on the person named in the application for the emergency intercept under prescribed circumstances.

Under Florida law, there is no similar "emergency intercept" provision.

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 state law authorizing such wiretaps under s. 934.07, F.S.

Assistance From Communications Service Providers
Communications service providers and their employees, landlords, custodians and other persons must provide information, facilities or technical assistance in emergency interception of communications or electronic surveillance, if they have received written certification from the U.S. Attorney General or other authorized persons to conduct such interception or surveillance. The written certification must state that no warrant or court order is required by law, that all statutory requirements have been met and that the persons' or entities' assistance is required by law. 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

Federal law authorizes the installation and use of a pen register or a trap and trace device. *See* 18 U.S.C. 3125 specifically provides authorization for the installation and use of a pen register or a trap and trace device. The authorization procedures are essentially the same as those for securing an emergency intercept. 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.

A "pen register"[2] 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. For example, a pen register might be used on a suspected drug dealer's phone line to provide investigators with leads as to the dealer's suppliers and customers. 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).

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. This device is used in a variety of situations including when investigators know

[2]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."

an extortionist or kidnapper makes a demand over a particular phone. Pursuant to a request from a federal government attorney or a law enforcement officer authorized by 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. *See* 18 U.S.C. 3124(b).

Government 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: 1) 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 2) in the case of a state governmental authority, such order is not otherwise prohibited by state law;

- Has the subscriber's or customer's consent 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 is engaged in telemarketing. 18 U.S.C. 2703(c)(1)(B).

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

Disclosure by Communications Service Providers
Providers of electronic communication services or remote computer services are required to disclose the following information to a governmental entity upon the issuance of 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:

- 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 similar records disclosure provision as 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 legal and illegal wiretapping of wire, oral, and electronic communications into some parity 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 and install pen registers or trap and trace devices under specified circumstances, including emergency situations without prior court approval. A section-by-section analysis follows:

Section 1 amends s. 934.02, F.S., relating to applicable definitions, to revise several terms. 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*, replaces the term "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 for *electronic communication* is amended to parallel an identical exemption in federal law for electronic funds transfer information stored by a financial institution within the definition of "electronic communication" in 18 U.S.C. 2510(12). Electronic funds transfers are covered under other provisions relating to stored electronic communications.

Section 2 amends s. 934.03, F.S., relating to illegal interception and disclosure of wire, oral and electronic communications, to:

- Create a third degree felony for the intentional disclosure of the contents of a legally authorized communications interception to an unauthorized party which is consistent with a similar criminal offense provision in 18 U.S.C. 2511(1)(e). [Since no time frame is imposed relating to when a disclosure is made, this provision may subject someone to prosecution for disclosure years after the denial of the application for and a termination of a wiretap.]

- Amend the misdemeanor penalty provisions to include reference to cordless telephones for the purpose of applying penalty provisions which is consistent with similar penalty provisions in 18 U.S.C. 2511(4)(a)-(b).

- Add the term "electronic communications" to the list of communications that may be intercepted by service providers while engaged in any activity that is a necessary incident to the rendition of the provider's service or to the protection of the service provider's rights or property which is consistent with a similar provision in 18 U.S.C. 2511(2)(a)(I).

- Allows a provider of a wire, oral, or electronic communication service and other designated persons to provide information, facilities, or technical assistance to a person legally authorized to intercept such communications if the provider or other designated person receives written certification from the authorized person that no warrant or court

order is required by law to conduct the emergency intercept, 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 amends s. 934.07, F.S., relating to legal interception of wire, oral and electronic communications. The offense of prostitution is eliminated from the list of enumerated offenses for which a communications interception may be authorized. This is consistent with state court rulings. *See State v. Rivers*, 660 So.2d 1360 (Fla. 1995)(federal law pre-empted state law authority such that the wiretap law does not authorize the use of wiretaps to investigate nonviolent prostitution-related offenses). The enumerated list of offenses under the federal law are not identical to the listing under Florida law (s. 18 U.S.C. 2517).

Section 4 amends s. 934.09, F.S., relating to the procedure for interception of wire, oral, and electronic communications. An "emergency intercept" provision is created based on federal law (see 18 U.S.C. 2518(7)). An investigator or law enforcement officer, specially designated by the Governor, the Attorney General or the statewide prosecutor or state attorney[3], may initiate an emergency intercept without prior court approval, provided that the court approval must be secured within 48 hours after the interception is initiated. Such authorized person must reasonably determine beforehand that:

- An emergency exists which involves: 1) immediate danger of death, 2) serious physical injury to any person or 3) escape of a prisoner[4]; and
- A wire, oral, or electronic communication must 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.

These emergency intercept provisions differ from the federal emergency intercept provision in three ways. First, unlike the federal law, the bill does not include "conspiratorial activities threatening the national security" or "conspiratorial activities characteristic of organized crime" as bases for an emergency intercept. Second, unlike the federal law, the bill refers to "immediate danger of death or serious bodily injury" in lieu of "the immediate danger of death or serious

[3]This is a broader category of authorized persons than those authorized to apply for court-approved interceptions of communications. However, such officers must be specially designated by the Governor in order to apply for an emergency interception of communications.

[4]The terms "danger of escape of a prisoner" and "prisoner" are undefined, therefore it is not known what the scope of application would be. A definition for prisoner is found in s. 57.085, F.S., relating to the waiver of court costs for a prisoner who is defined as someone who has been convicted of a crime and is incarcerated for that crime or who is being held in custody pending extradition or sentencing. County and municipal prisoners are more specifically defined in chapter 951, F.S., relating to county and municipal prisoners. *See* s. 951.23(1)(c) and (e), F.S. The "escape of a prisoner" is a second degree felony under section 944.40, F.S., which applies to any prisoner who escapes or attempts to escape and who was confined in any prison, jail, private correctional facility, road camp, or other penal institution, whether operated by the state, a county, or a municipality, or operated under a contract with the state, a county, or a municipality, working upon the public roads, or being transported to or from a place of confinement.

physical injury." Third, unlike the federal law, the bill does include the "escape of a prisoner" as a basis for an emergency intercept.

This section also provides that if an application for approval is denied or any other case in which the interception terminates without the issuance of an order, the contents of the intercepted wire, oral or electronic communication shall be treated as having been obtained in violation of s. 934.03(4) and an inventory must be served on the person or persons who were the subject of the interception within 90 days after the termination of the interception.

Other changes relating to the specificity of an application for an interception to a wire or electronic communication mirrors language in recent amendments to the federal wiretapping law in P.L. 105-272. For example, an adequate showing of probable cause that a person's actions could have the effect of thwarting interception from a specified facility must be made in an application for the interception of a wire or electronic communication. In addition, an order authorizing or approving an interception must be narrowly tailored in time to the communication at issue.

Section 5 amends s. 934.10, F.S., relating to civil actions brought by any person for wrongful interception or disclosure of wireless, oral or electronic communications under ss. 934.03-934.09, F.S. It expands the good faith reliance defense to include reliance based on a request of an investigative or law enforcement officer under the new emergency intercept provisions. This provision is similar to the federal provision in 18 U.S.C. 2520(d)(2).

This section, however, pre-empts federal law by requiring the consent of all parties in lieu of the consent of one-party, as permitted by federal law, to a communications for purposes of asserting the defense of good faith reliance.

Section 6 amends s. 934.23, F.S., relating to governmental access to electronic records of communications. This section specifies the types of information a service provider must disclose when subpoenaed by an investigative or law enforcement officers, to include 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 existing federal provisions in 18 U.S.C. 2703(c)(1)(B) and (C), (c)(2), (d), and (f). 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 amends s. 934.27, F.S., relating to civil actions brought by providers of electronic communication service or a subscriber or customer, for disclosure of electronic records arising under ss. 934.21-934.28. It expands the good faith reliance defense to include reliance based on a request of an investigative or law enforcement officer under the 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 amends s. 943.31, F.S., relating to the legal and illegal use of pen registers and trap and trace devices. This section provides 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 identical to the federal provision in 18 U.S.C. 3121(c).

In addition, this section creates new provisions relating to the emergency installation and use of pen registers and trap and trace devices without prior court approval. This provision is analogous to the provisions for the emergency intercept of communications under s. 934.09, F.S., including the same circumstances as bases for initiating an emergency installation and use of pen registers.

A service provider and others who furnished facilities or technical assistance must be 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 with the same exceptions noted for the emergency intercept provisions in section 9 of the bill.

Section 9 amends s. 934.34, F.S., relating to mandatory assistance in the installation and use of pen registers and trap and trace devices. It specifies 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 to conduct an emergency pen register or trap and trace installation under the new provisions. The provisions are similar to federal provisions in 18 U.S.C. 3124(b).

Section 10 provides that the effective date of the bill is October 1, 2001.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. Other Constitutional Issues:

The Florida Supreme Court has held that the express right of privacy in section 23 of article I of the Florida Constitution provides broader protection than that afforded by the U.S. Constitution. *See* *Winfield v. Division of Pari-Mutual Wagering*, 477 So.2d 544 (Fla. 1985). Therefore, any state regulation of a fundamental right is subject to the higher standard of review, i.e., strict scrutiny. This recognition is exemplified in Florida's wiretap law which, unlike federal law, requires all parties to a communication to consent to the interception under the circumstances provided. In addition, Florida's wiretap law already contains a separate statutory provision that expressly prohibits the use of intercepted wire or oral

communications obtained in violation of chapter 934, F.S., but it does not contain such prohibition for information obtained from pen registers or trap and trace devices in violation of chapter 934, F.S. *See* s. 934.06, F.S. There is concern that the absence of similar protective exclusionary language for information obtained from emergency wiretapping using pen registers or trap and trace devices may conflict with an individual's constitutionally protected right of privacy and due process considerations since these types of wiretaps are obtained without prior court approval.

V. Economic Impact and Fiscal Note:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

The bill may benefit the public by providing law enforcement with additional means to access information directly or indirectly related to criminal activity. However, it also limits civil liberties or expectations of privacy for specified circumstances under which authorized persons reasonably determine warrant emergency interception or emergency installation of communications wiretap devices.

The bill will also benefit communications services providers by providing them with civil and criminal immunity for assisting law enforcement and by compensating them for their assistance.

C. Government Sector Impact:

This bill expands law enforcement authority to conduct interception of communications and installation of pen registers and trap and trace devices under specified circumstances. It also provides law enforcement with broader civil and criminal immunity for acting in good faith reliance under the bill.

VI. Technical Deficiencies:

None.

VII. Related Issues:

- Unlike the new provision relating to the emergency interception of communications, the provision for an emergency installation of pen registers and trap and trace devices does not contain language to limit the use or admissibility of information obtained or derived if the subsequent application, within 48 hours, to the court is denied or if the installation terminates without the issuance of a court order. Notably, a limitation on the use or admissibility of information obtained to emergency installation of pen registers or trap and trace devices is contained in the most recent federal law relating to such installation in foreign intelligence and international terrorism investigations. *See e.g.*, 50 U.S.C. 1843 (P.L. 105-272).

VIII. Amendments:

None.