By Representative Gelber

A bill to be entitled

An act relating to the interception of communications; amending s. 934.02, F.S.; revising definitions; including wire communications within the meaning of an electronic communications system; redefining the terms "pen register" and "trap and trace device"; defining the terms "foreign intelligence information," "protected computer," and "computer trespasser"; amending s. 934.03, F.S.; authorizing the interception of certain wire or electronic communications of a computer trespasser; amending s. 934.07, F.S.; authorizing the Department of Law Enforcement to intercept wire, oral, or electronic communications for purposes of investigating certain additional offenses concerning terrorism and the attempted or threatened use of a destructive device or weapon of mass destruction; requiring a law enforcement agency to notify the Department of Law Enforcement if an intercepted communication provides evidence of certain acts of terrorism; amending s. 934.09, F.S.; providing for the interception of communications upon certain findings of activities that threaten the security of the nation or state; specifying circumstances under which the court may authorize the interception of communications outside the court's jurisdiction; amending s. 934.08, F.S.; authorizing the disclosure of the

contents of an intercepted communication to certain state and federal officials; amending s. 934.22, F.S.; prohibiting a provider of electronic communication service or a provider of remote computing service from disclosing the contents of communications or information pertaining to a subscriber or customer; specifying certain exceptions; amending s. 934.23, F.S.; providing for disclosure of information pertaining to a subscriber or customer under specified circumstances and pursuant to a warrant; amending s. 934.27, F.S.; providing that a request of an investigative or law enforcement officer to preserve records is a defense with respect to a civil or criminal action concerning unlawful access to communications; amending s. 934.31, F.S.; prohibiting the recording of the contents of communications by the use of a pen register or trap and trace device; amending s. 934.33, F.S.; requiring that a certification of an order for a pen register or a trap and trace device be provided to any person or entity not specifically named in the order; requiring that the order include information concerning location of the device and geographic limits of the order; requiring an investigative or law enforcement agency to maintain a record of the use of a pen register or trap and trace device installed pursuant to an ex parte order; requiring that the record be provided to the

court; amending s. 934.34, F.S.; providing for a trap and trace device to be installed on other facilities; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Subsections (1), (8), (14), (20), and (21) of section 934.02, Florida Statutes, are amended, and subsections (24), (25), and (26) are added to said section, to read:

934.02 Definitions.--As used in this chapter:

(1) "Wire communication" means 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 intrastate, interstate, or foreign communications or communications affecting intrastate, interstate, or foreign commerce. ~~Such term includes any electronic storage of such communication.~~

(8) "Judge of competent jurisdiction" means justice of the Supreme Court, judge of a district court of appeal, circuit judge, or judge of any court of record having felony jurisdiction of the State of Florida, irrespective of the geographic location or jurisdiction where the judge presides.

(14) "Electronic communications system" means any wire, radio, electromagnetic, photooptical, or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related

electronic equipment for the electronic storage of such communications.

(20) "Pen register" means a device or process that ~~which~~ records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but such information does not include the contents of any communication. The ~~electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such~~ term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing or recording as an incident to billing or~~,~~ for communication services provided by such provider, and does not include ~~or~~ any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

(21) "Trap and trace device" means a device or process that ~~which~~ captures the incoming electronic or other impulses that ~~which~~ identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but such information does not include the contents of any communication ~~of an instrument or a device from which a wire or electronic communication was transmitted~~.

(24) "Foreign intelligence information" means information, whether or not concerning a United States person, as that term is defined in 50 U.S.C. s. 1801, which relates to:

(a) The ability of the United States to protect against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(b) Sabotage or international terrorism by a foreign power or an agent of a foreign power;

(c) Clandestine intelligence activities by an intelligence service, a network of a foreign power, or an agent of a foreign power; or

(d) With respect to a foreign power or foreign territory, the national defense or security of the United States or the conduct of the foreign affairs of the United States.

(25) "Protected computer" means:

(a) A computer for the exclusive use of a financial institution or governmental entity;

(b) A computer that is not for the exclusive use of a financial institution or governmental entity, but that is used by or for a financial institution or governmental entity and with respect to which unlawful conduct can affect the use by or for the financial institution or governmental entity; or

(c) A computer that is used in interstate or foreign commerce or communication, including a computer located outside the United States.

(26) "Computer trespasser" means a person who accesses a protected computer without authorization and thus does not have a reasonable expectation of privacy with respect to any communication transmitted to, through, or from the protected computer. The term does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator

of the protected computer for access to all or part of the protected computer.

Section 2. Paragraph (j) is added to subsection (2) of section 934.03, Florida Statutes, to read:

934.03 Interception and disclosure of wire, oral, or electronic communications prohibited.--

(2)

(j) It is not unlawful under ss. 934.03-934.09 for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser which are transmitted to, through, or from a protected computer if:

1. The owner or operator of the protected computer authorizes the interception of the communications of the computer trespasser;

2. The person acting under color of law is lawfully engaged in an investigation;

3. The person acting under color of law has reasonable grounds to believe that the contents of the communications of the computer trespasser will be relevant to the investigation; and

4. The interception does not acquire communications other than those transmitted to, through, or from the computer trespasser.

Section 3. Section 934.07, Florida Statutes, as amended by section 1 of chapter 2001-359, Laws of Florida, is amended to read:

934.07 Authorization for interception of wire, oral, or electronic communications.--

(1) The Governor, the Attorney General, the statewide prosecutor, or any state attorney may authorize an application to a judge of competent jurisdiction for, and such judge may

grant in conformity with ss. 934.03-934.09 an order authorizing or approving the interception of, wire, oral, or electronic communications by:

(a) The Department of Law Enforcement or any law enforcement agency as defined in s. 934.02 having responsibility for the investigation of the offense as to which the application is made when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, aircraft piracy, arson, gambling, robbery, burglary, theft, dealing in stolen property, criminal usury, bribery, or extortion; any felony violation of ss. 790.161-790.166, inclusive;any violation of chapter 893; any violation of the provisions of the Florida Anti-Fencing Act; any violation of chapter 895; any violation of chapter 896; any violation of chapter 815; any violation of chapter 847; any violation of s. 827.071; any violation of s. 944.40; or any conspiracy or solicitation to commit any violation of the laws of this state relating to the crimes specifically enumerated in this paragraph.

(b) The Department of Law Enforcement, together with other assisting personnel as authorized and requested by the department under s. 934.09(5), for the investigation of the offense as to which the application is made when such interception may provide or has provided evidence of the commission of any offense that may be an act of terrorism or in furtherance of an act of terrorism or evidence of any conspiracy or solicitation to commit any such violation.

(2)(a) If, during the course of an interception of communications by a law enforcement agency as authorized under paragraph (1)(a), the law enforcement agency finds that the intercepted communications may provide or have provided

evidence of the commission of any offense that may be an act of terrorism or in furtherance of an act of terrorism, or evidence of any conspiracy or solicitation to commit any such violation, the law enforcement agency shall promptly notify the Department of Law Enforcement and apprise the department of the contents of the intercepted communications. The agency notifying the department may continue its previously authorized interception with appropriate minimization, as applicable, and may otherwise assist the department as provided in this section.

(b) Upon its receipt of information of the contents of an intercepted communications from a law enforcement agency, the Department of Law Enforcement shall promptly review the information to determine whether the information relates to an actual or anticipated act of terrorism as defined in this section. If, after reviewing the contents of the intercepted communications, there is probable cause that the contents of the intercepted communications meet the criteria of paragraph (1)(b), the Department of Law Enforcement may make application for the interception of wire, oral, or electronic communications consistent with subsection (1)(b). The department may make an independent new application for interception based on the contents of the intercepted communications. Alternatively, the department may request the law enforcement agency that provided the information to join with the department in seeking an amendment of the original interception order, or may seek additional authority to continue intercepting communications under the direction of the department. In carrying out its duties under this section, the department may use the provisions for an emergency

interception provided in s. 934.09(7) if applicable under statutory criteria.

(3)~~(2)~~ As used in this section, the term "terrorism" means an activity that:

(a)1. Involves a violent act or an act dangerous to human life which is a violation of the criminal laws of this state or of the United States; or

2. Involves a violation of s. 815.06; and

(b) Is intended to:

1. Intimidate, injure, or coerce a civilian population;

2. Influence the policy of a government by intimidation or coercion; or

3. Affect the conduct of government through destruction of property, assassination, murder, kidnapping, or aircraft piracy.

Section 4. Subsection (7) and paragraph (b) of subsection (11) of section 934.09, Florida Statutes, as amended by section 2 of chapter 2001-359, Laws of Florida, are amended to read:

934.09 Procedure for interception of wire, oral, or electronic communications.--

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer specially designated by the Governor, the Attorney General, the statewide prosecutor, or a state attorney acting under this chapter, who reasonably determines that:

(a) An emergency exists that:

1. Involves immediate danger of death or serious physical injury to any person, ~~or~~ the danger of escape of a

prisoner, or conspiratorial activities threatening the security interest of the nation or state; and

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

(b) There are grounds upon which an order could be entered under this chapter to authorize such interception

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within 48 hours after the interception has occurred or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. If such application for approval 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 shall be treated as having been obtained in violation of s. 934.03(4), and an inventory shall be served as provided for in paragraph (8)(e) on the person named in the application.

(11) The requirements of subparagraph (1)(b)2. and paragraph (3)(d) relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if:

(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 that 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 that 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 that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

Consistent with this paragraph, a judge of competent jurisdiction ~~and limited to investigations of acts of terrorism, as that term is defined in s. 934.07, the court~~ may authorize ~~continued~~ interception within this state, whether the interception is ~~both~~ within or ~~and~~ outside the court's ~~its~~ jurisdiction, if the application for the interception makes a showing that some activity or conspiracy believed to be related to, or in furtherance of, the criminal predicate for the requested interception has occurred or will likely occur, in whole or in part, within the jurisdiction of the court where the order is being sought ~~original interception occurred within its jurisdiction~~.

Section 5. Effective July 1, 2004, paragraph (b) of subsection (11) of section 934.09, Florida Statutes, as amended by this act and by section 3 of chapter 2001-359, Laws of Florida, is amended to read:

934.09 Procedure for interception of wire, oral, or electronic communications.--

(11) The requirements of subparagraph (1)(b)2. and paragraph (3)(d) relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if:

(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 that 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 that 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 that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

Consistent with this paragraph, a judge of competent jurisdiction may authorize interception within this state, whether the interception is within or outside the court's jurisdiction, if the application for the interception makes a showing that some activity or conspiracy believed to be related to, or in furtherance of, the criminal predicate for the requested interception has occurred or will likely occur, in whole or in part, within the jurisdiction of the court where the order is being sought.

Section 6. Subsection (1) of section 934.08, Florida Statutes, is amended to read:

934.08 Authorization for disclosure and use of intercepted wire, oral, or electronic communications.--

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may disclose such contents to:

(a) The Department of Legal Affairs for use in investigations or proceedings pursuant to s. 812.035, part II of chapter 501, chapter 542, or chapter 895, to any attorney authorized by law to investigate and institute any action on behalf of the State of Florida or political subdivision thereof, or to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer or person making or receiving the disclosure.

(b) Any state or federal law enforcement official, state or federal intelligence official, state or federal protective services official, federal immigration official,

state or federal defense official, or state or federal security official to the extent that the contents or evidence includes foreign intelligence or counterintelligence, as defined in 50 U.S.C. s. 401a, or foreign intelligence information, as defined in this chapter, in order to assist the official who receives that information in performing his or her official duties. Any state or federal official who receives information under this subsection may use that information only as necessary in conducting official duties and is subject to any limitations on the unauthorized disclosure of such information.

Section 7. Section 934.22, Florida Statutes, is amended to read:

934.22 Voluntary disclosure of customer communications or records ~~contents~~.--

(1) Except as provided in subsection (2) or subsection (3):

(a) A provider of ~~person or entity who provides an~~ electronic communication service to the public may not knowingly divulge to:

1. Any person or entity the contents of a communication while in electronic storage by that service; or~~.~~

2. Any governmental entity a record or other information pertaining to a subscriber to or customer of such service.

(b) A provider of ~~person or entity who provides~~ remote computing service to the public may not knowingly divulge to:

1. Any person or entity the contents of any communication that ~~which~~ is carried or maintained on that service:

a.~~1.~~ On behalf of a subscriber or customer of such service and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of such remote computing service; and ~~or~~

b.~~2.~~ Solely for the purpose of providing storage or computer processing services to its subscriber or customer, if the provider is not authorized to access the contents of any such communication for purposes of providing any service other than storage or computer processing; or~~.~~

2. Any governmental entity a record or other information pertaining to a subscriber to or customer of such service.

(2) A provider described in subsection (1)~~person or entity~~ may divulge the contents of a communication:

(a) To an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) As otherwise authorized in s. 934.03(2)(a), s. 934.07, or s. 934.23.

(c) With the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of a remote computing service.

(d) To a person employed or authorized, or whose facilities are used, to forward such communication to its destination.

(e) As may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service.

(f) To a law enforcement agency, if ~~such contents~~:

1. The contents were inadvertently obtained by the service provider;~~, and~~

2. The contents appear to pertain to the commission of a crime; or~~.~~

3. The provider reasonably believes an emergency involving immediate danger of death or serious physical injury to another person requires disclosure of the contents without delay.

(3)(a) A provider described in subsection (1) may disclose a record or other information pertaining to a subscriber to or customer of such service:

1. As is otherwise authorized in s. 934.23.

2. With the lawful consent of the customer or subscriber.

3. As is necessary incident to rendering service or protecting the rights or property of the provider of that service.

4. To a governmental entity if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information.

5. To any person other than a governmental entity.

(b) Notwithstanding paragraph (a), a provider may not disclose the contents of communications specified in paragraph (1)(a) or paragraph (1)(b).

Section 8. Section 934.23, Florida Statutes, is amended to read:

934.23 Required disclosure of customer communications or records ~~Requirements for governmental access~~.--

(1) An investigative or law enforcement officer may require the disclosure by a provider of electronic

communication service of the contents of a wire or ~~an~~ electronic communication that has been in electronic storage in an electronic communications system for 180 days or less only pursuant to a warrant issued by the judge of a court of competent jurisdiction. An investigative or law enforcement officer may require the disclosure by a provider of electronic communication services of the contents of a wire or ~~an~~ electronic communication that has been in electronic storage in an electronic communications system for more than 180 days by the means available under subsection (2).

(2) An investigative or law enforcement officer may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this subsection is made applicable by subsection (3):

(a) Without required notice to the subscriber or customer if the investigative or law enforcement officer obtains a warrant issued by the judge of a court of competent jurisdiction; or

(b) With prior notice, or with delayed notice pursuant to s. 934.25, from the investigative or law enforcement officer to the subscriber or customer if the investigative or law enforcement officer:

1. Uses a subpoena; or

2. Obtains a court order for such disclosure under subsection (5).

(3) Subsection (2) is applicable with respect to any electronic communication that is held or maintained on a remote computing service:

(a) On behalf of a subscriber or customer of such service and received by means of electronic transmission from, or created by means of computer processing of communications

received by means of electronic transmission from, a subscriber or customer of such service.

(b) Solely for the purposes of providing storage or computer processing services to a subscriber or customer, if the provider is not authorized to access the contents of any such communication for purposes of providing any service other than storage or computer processing.

(4)(a) An investigative or law enforcement officer may require ~~Except as provided in paragraph (b),~~ a provider of electronic communication service or remote computing service to ~~may~~ disclose a record or other information pertaining to a subscriber or customer of such service, not including the contents of a communication, ~~covered by subsection (1) or subsection (2), to any person other than an investigative or law enforcement officer.~~

~~(b) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service, not including the contents of communications covered by subsection (1) or subsection (2), to an investigative or law enforcement officer~~ only when the investigative or law enforcement officer:

1. Obtains a warrant issued by the judge of a court of competent jurisdiction;

2. Obtains a court order for such disclosure under subsection (5); ~~or~~

3. Has the consent of the subscriber or customer to such disclosure; or~~.~~

4. Seeks information under paragraph (b).

(b)~~(c)~~ A provider of electronic communication service or remote computing service shall disclose to an investigative

or law enforcement officer the name;~~,~~address; local and long distance telephone connection records, or records of session times or durations; length of service, including the starting date of service; types of services used; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment, including any credit card or bank account number of~~, telephone toll billing records, telephone number or other subscriber number or identity, and length of service as~~ a subscriber to or customer of such service ~~and the types of services the subscriber or customer used~~ when the governmental entity uses a subpoena or obtains such information in the manner specified in paragraph (a) for obtaining information under that paragraph.

(c)~~(d)~~ An investigative or law enforcement officer who receives records or information under this subsection is not required to provide notice to a subscriber or customer.

(5) A court order for disclosure under subsection (2), subsection (3), or subsection (4) shall issue only if the investigative or law enforcement officer offers specific and articulable facts showing that there are reasonable grounds to believe the contents of a wire or electronic communication or the records of other information sought are relevant and material to an ongoing criminal investigation. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(6) No cause of action shall lie in any court against any provider of wire or electronic communication service, its

officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under ss. 934.21-934.28.

(7)(a) A provider of wire or electronic communication services or a remote computing service, upon the request of an investigative or law enforcement officer, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(b) Records referred to in paragraph (a) shall be retained for a period of 90 days, which shall be extended for an additional 90 days upon a renewed request by an investigative or law enforcement officer.

(8) A provider of electronic communication service, a remote computing service, or any other person who furnished assistance pursuant to this section shall be held harmless from any claim and civil liability resulting from the disclosure of information pursuant to this section and shall be reasonably compensated for reasonable expenses incurred in providing such assistance.

Section 9. Subsection (4) of section 934.27, Florida Statutes, is amended to read:

934.27 Civil action: relief; damages; defenses.--

(4) A good faith reliance on any of the following is a complete defense to any civil or criminal action brought under ss. 934.21-934.28:

(a) A court warrant or order, a subpoena, or a statutory authorization<u>, including, but not limited to, a request of an investigative or law enforcement officer to</u>

preserve records or other evidence, as provided in s. 934.23(7).

(b) A request of an investigative or law enforcement officer under s. 934.09(7).

(c) A good faith determination that s. 934.03(3) permitted the conduct complained of.

Section 10. Subsections (3) and (4) of section 934.31, Florida Statutes, are amended to read:

934.31 General prohibition on pen register and trap and trace device use; exception.--

(3) An investigative or law enforcement officer authorized to install and use a pen register or trap and trace device under ss. 934.31-934.34 shall use technology reasonably available to him or her which restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information used in processing and transmitting wire or electronic communications so that the contents of any wire or electronic communications are not recorded or decoded ~~call processing~~.

(4)(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer specially designated by the Governor, the Attorney General, the statewide prosecutor, or a state attorney acting pursuant to this chapter, who reasonably determines that:

1. An emergency exists which:

a. Involves immediate danger of death or serious physical injury to any person or the danger of escape of a prisoner, or involves conspiratorial activities threatening the security interest of the nation or state; and

b. Requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained; and

2. There are grounds upon which an order could be entered under this chapter to authorize such installation and use,

may have installed and use a pen register or trap and trace device if, within 48 hours after the installation has occurred or begins to occur, an order approving the installation or use is issued in accordance with s. 934.33.

(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied, or when 48 hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to paragraph (a) without application for the authorizing order within 48 hours after the installation constitutes a violation of s. 934.31.

(d) A provider of wire or electronic service, landlord, custodian, or other person who has furnished facilities or technical assistance pursuant to this subsection shall be held harmless from any claims and civil liability resulting from the disclosure of information pursuant to this subsection and shall be reasonably compensated for reasonable expenses incurred in providing such facilities and assistance.

Section 11. Section 934.33, Florida Statutes, is amended to read:

934.33 Issuance of an order for a pen register or a trap and trace device.--

(1) Upon application made under s. 934.32, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the applicant specified in s. 934.32(1) has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. Whenever such order is served on any person or entity not specifically named in the order, upon request of such person or entity, the person specified in s. 934.32 who has requested and is serving such order shall provide written or electronic certification that such order applies to the person or entity being served.

(2) An order issued under this section:

(a) Must specify the following:

1. The identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied.

2. The identity, if known, of the person who is the subject of the criminal investigation.

3. The attributes of the communications to which the order applies, including the number or other identifier and, if known, the ~~physical~~ location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of an order authorizing installation and use of a trap and trace device, the geographic limits of the ~~trap and trace~~ order.

4. A statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.

(b) Must direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under s. 934.34.

(3)(a) An order issued under this section may not authorize the installation and use of a pen register or a trap and trace device for more than 60 days.

(b) Extensions of such an order may be granted but only upon an application for an order under s. 934.32 and upon the judicial finding required by subsection (1). The period of extension may not exceed 60 days.

(4) An order authorizing or approving the installation and use of a pen register or a trap and trace device must direct that:

(a) The order be sealed until otherwise ordered by the court, and

(b) The person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached or applied, or who is obligated by the order ~~has been ordered by the court~~ to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber or to any other person except as otherwise ordered by the court.

(5) A court may not require greater specificity or additional information beyond that which is required under s. 934.32 and this section as a requisite for issuing an order as provided in this section.

(6)(a) If an investigative or law enforcement agency implementing an ex parte order under this section seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency must ensure that a record is maintained which identifies:

1. Each officer who installed the device and each officer who accessed the device to obtain information from the network;

2. The date and time the device was installed; the date and time the device was uninstalled; and the date, time, and duration of each occasion the device was accessed to obtain information;

3. The configuration of the device at the time of its installation and any subsequent modification of that configuration; and

4. Any information that was collected by the device.

(b) To the extent that the pen register or trap and trace device can be set automatically to record electronically the information required in paragraph (a), the record shall be maintained electronically throughout the installation and use of the device.

(7) The record maintained under subsection (6) shall be provided ex parte and under seal to the court that entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order, including any extension of the order.

Section 12. Subsection (2) of section 934.34, Florida Statutes, is amended to read:

934.34 Assistance in installation and use of a pen register or a trap and trace device.--

(2) Upon the request of the applicant specified in s. 934.32(1), a provider of a wire or electronic communication service, landlord, custodian, or other person shall install a trap and trace device forthwith on the appropriate line or other facility and shall furnish such investigative or law enforcement officer or other applicant all additional information, facilities, and technical assistance, including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place if such installation and assistance is directed by a court order as provided in s. 934.33(2)(b). Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to s. 934.31(4) or s. 934.33(2)(b), to an officer of the law enforcement agency designated in the court order at reasonable intervals during regular business hours for the duration of the order. The obligation of a provider of electronic communication service under such an order or under such emergency pen register or trap and trace device installation may include, but is not limited to, conducting an in-progress trace, or providing other assistance to support the investigation as may be specified in the order.

Section 13. This act shall take effect upon becoming a law.

****

LEGISLATIVE SUMMARY

Revises various laws governing the interception of communications by investigative or law enforcement agencies. Defines the terms "foreign intelligence information," "protected computer," and "computer trespasser." Authorizes a law enforcement agency to intercept wire or electronic communications of a computer trespasser. Authorizes the Department of Law Enforcement to intercept wire, oral, or electronic communications for purposes of investigating acts of terrorism or the attempted or threatened use of a destructive device or weapon of mass destruction. Provides for a court to authorize the interception of communications outside the court's jurisdiction. Authorizes a law enforcement agency to disclose the contents of an intercepted communication to certain state and federal officials. Provides that the request of a law enforcement officer to preserve records is a defense against a civil or criminal action concerning unlawful access to communications. Provides certain limitations on the use of a pen register or trap and trace device. Requires that a law enforcement agency maintain a record of the use of a pen register or trap and trace device installed pursuant to an ex parte order. (See bill for details.)