

Select Year:

The 2011 Florida Statutes

[Title XLVII](#)[Chapter 934](#)[View Entire Chapter](#)

CRIMINAL PROCEDURE AND CORRECTIONS SECURITY OF COMMUNICATIONS

CHAPTER 934

SECURITY OF COMMUNICATIONS

- 934.01 Legislative findings.
- 934.02 Definitions.
- 934.03 Interception and disclosure of wire, oral, or electronic communications prohibited.
- 934.04 Manufacture, distribution, or possession of wire, oral, or electronic communication intercepting devices prohibited.
- 934.05 Confiscation of wire, oral, or electronic communication intercepting devices.
- 934.06 Prohibition of use as evidence of intercepted wire or oral communications; exception.
- 934.07 Authorization for interception of wire, oral, or electronic communications.
- 934.08 Authorization for disclosure and use of intercepted wire, oral, or electronic communications.
- 934.09 Procedure for interception of wire, oral, or electronic communications.
- 934.10 Civil remedies.
- 934.15 Situations in which law enforcement officer may order telephone line cut, rerouted, or diverted.
- 934.21 Unlawful access to stored communications; penalties.
- 934.215 Unlawful use of a two-way communications device.
- 934.22 Voluntary disclosure of customer communications or records.
- 934.23 Required disclosure of customer communications or records.
- 934.24 Backup preservation; customer notification; challenges by customer.
- 934.25 Delayed notice.
- 934.26 Cost reimbursement.
- 934.27 Civil action: relief; damages; defenses.
- 934.28 Exclusivity of remedies and sanctions.
- 934.31 General prohibition on pen register and trap and trace device use; exception.
- 934.32 Application for an order for a pen register or a trap and trace device.
- 934.33 Issuance of an order for a pen register or a trap and trace device.
- 934.34 Assistance in installation and use of a pen register or a trap and trace device.
- 934.41 Alternative penalty.
- 934.42 Mobile tracking device authorization.
- 934.43 Criminal disclosure of subpoena, order, or authorization.

934.01 Legislative findings.—On the basis of its own investigations and of published studies, the Legislature makes the following findings:

(1) Wire communications are normally conducted through the use of facilities which form part of an intrastate network. The same facilities are used for interstate and intrastate communications.

(2) In order to protect effectively the privacy of wire and oral communications, to protect the integrity of

court and administrative proceedings, and to prevent the obstruction of intrastate commerce, it is necessary for the Legislature to define the circumstances and conditions under which the interception of wire and oral communications may be authorized and to prohibit any unauthorized interception of such communications and the use of the contents thereof in evidence in courts and administrative proceedings.

(3) Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice.

(4) To safeguard the privacy of innocent persons, the interception of wire or oral communications when none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurance that the interception is justified and that the information obtained thereby will not be misused.

History.—s. 1, ch. 69-17.

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.

(2) “Oral communication” means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation and does not mean any public oral communication uttered at a public meeting or any electronic communication.

(3) “Intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

(4) “Electronic, mechanical, or other device” means any device or apparatus which can be used to intercept a wire, electronic, or oral communication other than:

(a) Any telephone or telegraph instrument, equipment, or facility, or any component thereof:

1. Furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

2. Being used by a provider of wire or electronic communications service in the ordinary course of its business or by an investigative or law enforcement officer in the ordinary course of her or his duties.

(b) A hearing aid or similar device being used to correct subnormal hearing to not better than normal.

(5) “Person” means any employee or agent of the State of Florida or political subdivision thereof, of the United States, or of any other state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.

(6) “Investigative or law enforcement officer” means any officer of the State of Florida or political subdivision thereof, of the United States, or of any other state or political subdivision thereof, who is empowered by law to conduct on behalf of the Government investigations of, or to make arrests for, offenses enumerated in this chapter or similar federal offenses, any attorney authorized by law to prosecute or participate in the prosecution of such offenses, or any other attorney representing the State of Florida or political subdivision thereof in any civil, regulatory, disciplinary, or forfeiture action relating to, based upon, or derived from such offenses.

(7) "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that 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.

(9) "Aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed.

(10) "Law enforcement agency" means an agency of the State of Florida or a political subdivision thereof or of the United States if the primary responsibility of the agency is the prevention and detection of crime or the enforcement of the penal, traffic, or highway laws of this state and if its agents and officers are empowered by law to conduct criminal investigations and to make arrests.

(11) "Communication common carrier" shall have the same meaning which is given the term "common carrier" in 47 U.S.C. s. 153(10).

(12) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects intrastate, interstate, or foreign commerce, but does not include:

- (a) Any wire or oral communication;
- (b) Any communication made through a tone-only paging device;
- (c) Any communication from an electronic or mechanical device which permits the tracking of the movement of a person or an object; or
- (d) Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

(13) "User" means any person or entity who:

- (a) Uses an electronic communication service, and
- (b) Is duly authorized by the provider of such service to engage in such use.

(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.

(15) "Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications.

(16) "Readily accessible to the general public" means, with respect to a radio communication, that such communication is not:

- (a) Scrambled or encrypted;
- (b) Transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
- (c) Carried on a subcarrier or other signal subsidiary to a radio transmission;
- (d) Transmitted over a communications system provided by a common carrier, unless the communication is a tone-only paging system communication; or
- (e) Transmitted on frequencies allocated under part 25; subpart D, subpart E, or subpart F of part 74; or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio.

(17) "Electronic storage" means:

- (a) Any temporary intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof.
- (b) Any storage of a wire or electronic communication by an electronic communication service for

purposes of backup protection of such communication.

(18) "Aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

(19) "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

(20) "Pen register" means a device or process that 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 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 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 captures the incoming electronic or other impulses that 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.

(22) "State" means any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, or any other possession or territory of the United States.

(23) "Subpoena" means any administrative subpoena authorized by federal or Florida law, federal or Florida grand jury subpoena, or any criminal investigative subpoena as authorized by Florida statute which may be utilized on behalf of the government by an investigative or law enforcement officer.

(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.

History.—s. 2, ch. 69-17; s. 1, ch. 72-294; s. 1, ch. 74-249; s. 1, ch. 80-27; s. 1, ch. 88-184; s. 1, ch. 89-269; s. 1581, ch. 97-102; s. 8, ch. 2000-369; s. 1, ch. 2002-72; s. 125, ch. 2010-5.

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

(1) Except as otherwise specifically provided in this chapter, any person who:

(a) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication;

(b) Intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

1. Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

2. Such device transmits communications by radio or interferes with the transmission of such communication;

(c) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) Intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication intercepted by means authorized by subparagraph (2)(a)2., paragraph (2)(b), paragraph (2)(c), s. 934.07, or s. 934.09 when that person knows or has reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, has obtained or received the information in connection with a criminal investigation, and intends to improperly obstruct, impede, or interfere with a duly authorized criminal investigation;

shall be punished as provided in subsection (4).

(2)(a)1. It is lawful under ss. 934.03-934.09 for an operator of a switchboard, or an officer, employee, or agent of a provider of 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 or her employment while engaged in any activity which is a necessary incident to the rendition of his or her 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.

2. Notwithstanding any other law, a provider of wire, oral, or electronic communication service, or an officer, employee, or agent thereof, or landlord, custodian, or other person, may provide information, facilities, or technical assistance to a person authorized by law to intercept wire, oral, or electronic communications if such provider, or an officer, employee, or agent thereof, or landlord, custodian, or other person, has been provided with:

a. A court order directing such assistance signed by the authorizing judge; or

b. A certification in writing by a person specified in s. 934.09(7) that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required.

3. A provider of wire, oral, or electronic communication service, or an officer, employee, or agent thereof, or landlord, custodian, or other person may not disclose the existence of any interception or the device used to accomplish the interception with respect to which the person has been furnished an order under ss. 934.03-934.09, except as may otherwise be required by legal process and then only after prior notice to the Governor, the Attorney General, the statewide prosecutor, or a state attorney, as may be appropriate. Any such disclosure renders such person liable for the civil damages provided under s. 934.10, and such person may be prosecuted under s. 934.43. An action may not be brought against any provider of wire, oral, or electronic communication service, or an officer, employee, or agent thereof, or landlord, custodian, or other person for

providing information, facilities, or assistance in accordance with the terms of a court order under ss. 934.03-934.09.

(b) It is lawful under ss. 934.03-934.09 for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his or her employment and in discharge of the monitoring responsibilities exercised by the commission in the enforcement of 47 U.S.C. ch. 5, to intercept a wire, oral, or electronic communication transmitted by radio or to disclose or use the information thereby obtained.

(c) It is lawful under ss. 934.03-934.09 for an investigative or law enforcement officer or a person acting under the direction of an investigative or law enforcement officer to intercept a wire, oral, or electronic communication when such person is a party to the communication or one of the parties to the communication has given prior consent to such interception and the purpose of such interception is to obtain evidence of a criminal act.

(d) It is lawful under ss. 934.03-934.09 for a person to intercept a wire, oral, or electronic communication when all of the parties to the communication have given prior consent to such interception.

(e) It is unlawful to intercept any wire, oral, or electronic communication for the purpose of committing any criminal act.

(f) It is lawful under ss. 934.03-934.09 for an employee of a telephone company to intercept a wire communication for the sole purpose of tracing the origin of such communication when the interception is requested by the recipient of the communication and the recipient alleges that the communication is obscene, harassing, or threatening in nature. The individual conducting the interception shall notify local police authorities within 48 hours after the time of the interception.

(g) It is lawful under ss. 934.03-934.09 for an employee of:

1. An ambulance service licensed pursuant to s. 401.25, a fire station employing firefighters as defined by s. 633.30, a public utility, a law enforcement agency as defined by s. 934.02(10), or any other entity with published emergency telephone numbers;
 2. An agency operating an emergency telephone number "911" system established pursuant to s. 365.171;
- or
3. The central abuse hotline operated pursuant to s. 39.201

to intercept and record incoming wire communications; however, such employee may intercept and record incoming wire communications on designated "911" telephone numbers and published nonemergency telephone numbers staffed by trained dispatchers at public safety answering points only. It is also lawful for such employee to intercept and record outgoing wire communications to the numbers from which such incoming wire communications were placed when necessary to obtain information required to provide the emergency services being requested. For the purpose of this paragraph, the term "public utility" has the same meaning as provided in s. 366.02 and includes a person, partnership, association, or corporation now or hereafter owning or operating equipment or facilities in the state for conveying or transmitting messages or communications by telephone or telegraph to the public for compensation.

(h) It shall not be unlawful under ss. 934.03-934.09 for any person:

1. To intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.
2. To intercept any radio communication which is transmitted:
 - a. By any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;
 - b. By any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including any police or fire communications system, readily accessible to the general public;
 - c. By a station operating on an authorized frequency within the bands allocated to the amateur, citizens

band, or general mobile radio services; or

d. By any marine or aeronautical communications system.

3. To engage in any conduct which:

a. Is prohibited by s. 633 of the Communications Act of 1934; or

b. Is excepted from the application of s. 705(a) of the Communications Act of 1934 by s. 705(b) of that act.

4. To intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station of consumer electronic equipment to the extent necessary to identify the source of such interference.

5. To intercept, if such person is another user of the same frequency, any radio communication that is not scrambled or encrypted made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system.

6. To intercept a satellite transmission that is not scrambled or encrypted and that is transmitted:

a. To a broadcasting station for purposes of retransmission to the general public; or

b. As an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, when such interception is not for the purposes of direct or indirect commercial advantage or private financial gain.

7. To intercept and privately view a private satellite video communication that is not scrambled or encrypted or to intercept a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted, if such interception is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain.

(i) It shall not be unlawful under ss. 934.03-934.09:

1. To use a pen register or a trap and trace device as authorized under ss. 934.31-934.34 or under federal law; or

2. For a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful, or abusive use of such service.

(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.

(3)(a) Except as provided in paragraph (b), a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication:

1. As otherwise authorized in paragraph (2)(a) or s. 934.08;

2. With the lawful consent of the originator or any addressee or intended recipient of such communication;

3. To a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

4. Which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b), whoever violates subsection (1) is guilty of a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, s. 775.084, or s. 934.41.

(b) If the offense is a first offense under paragraph (a) and is not for any tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) was committed is a radio communication that 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, then:

1. If the communication is not the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication, or a paging service communication, and the conduct is not that described in subparagraph (2)(h)7., the person committing the offense is guilty of a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

2. 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, a public land mobile radio service communication, or a paging service communication, the person committing the offense is guilty of a misdemeanor of the second degree, punishable as provided in s. 775.082 or s. 775.083.

History.—s. 3, ch. 69-17; s. 1163, ch. 71-136; ss. 2, 3, ch. 74-249; s. 249, ch. 77-104; s. 1, ch. 78-376; s. 187, ch. 79-164; s. 2, ch. 80-27; s. 1, ch. 87-301; s. 2, ch. 88-184; s. 2, ch. 89-269; s. 1582, ch. 97-102; s. 18, ch. 99-168; ss. 7, 9, ch. 2000-369; s. 2, ch. 2002-72; s. 30, ch. 2010-117.

934.04 Manufacture, distribution, or possession of wire, oral, or electronic communication intercepting devices prohibited.—

(1) Except as otherwise specifically provided in this chapter, any person who intentionally:

(a) Sends through the mail or otherwise sends or carries any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the illegal interception of wire, oral, or electronic communications as specifically defined by this chapter; or

(b) Manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the illegal interception of wire, oral, or electronic communications as specifically defined by this chapter;

shall be guilty of a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(2) It is not unlawful under this section for:

(a) A provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service; or

(b) An officer, agent, or employee of, or a person under contract with, bidding upon contracts with, or in the course of doing business with, the United States, a state, or a political subdivision thereof, in the normal course of the activities of the United States, a state, or a political subdivision thereof,

to send through the mail; send or carry in intrastate, interstate, or foreign commerce; or manufacture, assemble, possess, or sell any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

History.—s. 4, ch. 69-17; s. 1164, ch. 71-136; s. 3, ch. 88-184; s. 3, ch. 89-269.

934.05 Confiscation of wire, oral, or electronic communication intercepting devices.—Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, or sold in violation of this chapter may be seized and forfeited to the state.

History.—s. 5, ch. 69-17; s. 4, ch. 88-184.

934.06 Prohibition of use as evidence of intercepted wire or oral communications; exception.—Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the state, or a political subdivision thereof, if the disclosure of that information would be in violation of this chapter. The prohibition of use as evidence provided in this section does not apply in cases of prosecution for criminal interception in violation of the provisions of this chapter.

History.—s. 6, ch. 69-17; s. 4, ch. 89-269.

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 paragraph (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) 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.

History.—s. 7, ch. 69-17; ss. 11, 20, 35, ch. 69-106; s. 42, ch. 73-334; s. 1, ch. 77-174; s. 15, ch. 77-342; s. 33, ch. 79-8; s. 5, ch. 88-184; s. 5, ch. 89-269; s. 14, ch. 91-33; s. 10, ch. 2000-369; s. 1, ch. 2001-359; s. 3, ch. 2002-72.

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.

(2) 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 use such contents to the extent such use is appropriate to the proper performance of her or his official duties.

(3) Any person who has received, by any means authorized by this chapter, or by the laws of any other state or the United States, any information concerning a wire, oral, or electronic communication or evidence derived therefrom, intercepted in accordance with the provisions of this chapter, may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any criminal proceeding in any court of the state or of the United States; in any grand jury proceedings; in any proceeding pursuant to s. 812.035, part II of chapter 501, chapter 542, or chapter 895; in any investigation or

proceeding in connection with the Judicial Qualifications Commission; or in any other proceeding or investigation held under the authority of the State of Florida or any political subdivision thereof, of the United States, or of any other state or political subdivision thereof, if such testimony is otherwise admissible.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character, provided that a communication otherwise lawfully intercepted pursuant to this chapter is not privileged when such communication is in furtherance of the commission of a crime.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof and evidence derived therefrom may be disclosed or used as provided in subsections (1) and (2). Such contents and any evidence derived therefrom may be used under subsection (3) when authorized or approved by a judge of competent jurisdiction when such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

History.—s. 8, ch. 69-17; s. 2, ch. 72-294; s. 1, ch. 73-361; s. 6, ch. 88-184; s. 6, ch. 89-269; s. 1583, ch. 97-102; s. 6, ch. 2002-72.

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

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under ss. 934.03-934.09 shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) The identity of the investigative or law enforcement officer making the application and the officer authorizing the application.

(b) A full and complete statement of the facts and circumstances relied upon by the applicant to justify his or her belief that an order should be issued, including:

1. Details as to the particular offense that has been, is being, or is about to be committed.
2. Except as provided in subsection (11), a particular description of the nature and location of the facilities from which, or the place where, the communications are to be intercepted.
3. A particular description of the type of communications sought to be intercepted.
4. The identity of the person, if known, committing the offense and whose communications are to be intercepted.

(c) A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.

(d) A statement of the period of time for which the interception is required to be maintained and, if the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter.

(e) A full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application.

(f) When the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application, the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting, and outside such jurisdiction but within the State of Florida in the case of a mobile interception device authorized by the judge within such jurisdiction, if the judge determines on the basis of the facts submitted by the applicant that:

(a) There is probable cause for belief that an individual is committing, has committed, or is about to commit an offense as provided in s. 934.07.

(b) There is probable cause for belief that particular communications concerning that offense will be obtained through such interception.

(c) Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.

(d) Except as provided in subsection (11), 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 such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication shall specify:

(a) The identity of the person, if known, whose communications are to be intercepted.

(b) The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted.

(c) A particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates.

(d) The identity of the agency authorized to intercept the communications and of the person authorizing the application.

(e) The period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication shall, upon the request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. The obligation of a provider of wire, oral, or electronic communication service under such an order may include, but is not limited to, conducting an in-progress trace during an interception, or providing other assistance to support the investigation as may be specified in the order. Any provider of wire or electronic communication service, landlord, custodian, or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization or in any event longer than 30 days. Such 30-day period begins on the day on which the agent or officer of the law enforcement agency first begins to conduct an interception under the order or 10 days after the order is entered, whichever occurs earlier. Extensions of an order may be granted but only upon application for an extension made in accordance with subsection (1) and upon the court making the findings required by subsection (3). The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than 30 days. Every

order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under ss. 934.03-934.09, and must terminate upon attainment of the authorized objective or in any event in 30 days. If the intercepted communication is in code or foreign language and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under ss. 934.03-934.09 may be conducted in whole or in part by government personnel or by an individual operating under a contract with the government, acting under the supervision of an agent or officer of the law enforcement agency authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to ss. 934.03-934.09, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(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, 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.

(8)(a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by ss. 934.03-934.09 shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be kept in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his or her directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge, or that judge's successor in office, and in any event shall be kept for 10 years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of s. 934.08(1) and (2) for investigations.

(b) The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under s. 934.08(3), as required by federal law.

(c) Applications made and orders granted under ss. 934.03-934.09 shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. As required by federal law, such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and

shall not be destroyed except on order of the issuing or denying judge, or that judge's successor in office, and in any event shall be kept for 10 years.

(d) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(e) Within a reasonable time but not later than 90 days after the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his or her discretion to be in the interest of justice, an inventory which shall include notice of:

1. The fact of the entry of the order or the application.
2. The date of the entry and the period of authorized, approved, or disapproved interception, or the denial of the application.
3. The fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may make available to such person or the person's counsel for inspection such portions of the intercepted communications, applications, and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction, the serving of the inventory required by this paragraph may be postponed.

(9) As required by federal law, the contents of any intercepted wire, oral, or electronic communication or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding unless each party, not less than 10 days before the trial, hearing, or proceeding, has been furnished with a copy of the court order and accompanying application under which the interception was authorized or approved. This 10-day period may be waived by the judge if he or she finds that it was not possible to furnish the party with the above information 10 days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority may move to suppress the contents of any intercepted wire, oral, or electronic communication, or evidence derived therefrom, on the grounds that:

1. The communication was unlawfully intercepted;
2. The order of authorization or approval under which it was intercepted is insufficient on its face; or
3. The interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of ss. 934.03-934.09. The judge, upon the filing of such motion by the aggrieved person, may make available to the aggrieved person or his or her counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interest of justice.

(b) In addition to any other right to appeal, the state shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) or the denial of an application for an order of approval if the attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within 30 days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in ss. 934.03-934.10 with respect to the interception of electronic communications are the only judicial remedies and sanctions for violations of those sections involving such 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:

(a) In the case of an application with respect to the interception of an oral 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 contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted.
3. The judge finds that such specification is not practical.

(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, or the communication to be intercepted or expected to be intercepted is occurring or will likely occur, in whole or in part, within the jurisdiction of the court where the order is being sought.

(12) If an interception of a communication is to be carried out pursuant to subsection (11), such interception may not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided under paragraph (11)(b) may petition the court to modify or quash the order on the ground that the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the state, shall decide such a petition expeditiously.

History.—s. 9, ch. 69-17; s. 2, ch. 78-376; s. 7, ch. 88-184; s. 7, ch. 89-269; s. 1, ch. 94-101; s. 92, ch. 95-211; s. 1584, ch. 97-102; s. 11, ch. 2000-369; ss. 2, 3, ch. 2001-359; ss. 4, 5, ch. 2002-72.

934.10 Civil remedies.—

(1) Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of ss. 934.03-934.09 shall have a civil cause of action against any person or entity who intercepts, discloses, or uses, or procures any other person or entity to intercept, disclose, or use, such communications and shall be entitled to recover from any such person or entity which engaged in that violation such relief as may be appropriate, including:

- (a) Preliminary or equitable or declaratory relief as may be appropriate;
 - (b) Actual damages, but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher;
 - (c) Punitive damages; and
 - (d) A reasonable attorney's fee and other litigation costs reasonably incurred.
- (2) A good faith reliance on:

- (a) A court order, subpoena, or legislative authorization as provided in ss. 934.03-934.09,
- (b) A request of an investigative or law enforcement officer under s. 934.09(7), or
- (c) A good faith determination that Florida or federal law, other than 18 U.S.C. s. 2511(2)(d), permitted the conduct complained of

shall constitute a complete defense to any civil or criminal, or administrative action arising out of such conduct under the laws of this state.

(3) A civil action under this section may not be commenced later than 2 years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

History.—s. 10, ch. 69-17; s. 3, ch. 78-376; s. 8, ch. 88-184; s. 8, ch. 89-269; s. 12, ch. 2000-369.

934.15 Situations in which law enforcement officer may order telephone line cut, rerouted, or diverted.—

(1) The supervising law enforcement officer at the scene of an incident where there is reasonable cause to believe:

- (a) That a person is holding one or more hostages,
- (b) That a person has barricaded herself or himself and taken a position of confinement to avoid apprehension,
- (c) That there is the probability that a subject about to be arrested will resist with the use of weapons, or
- (d) That a person has barricaded herself or himself and is armed and is threatening suicide,

may order law enforcement or telephone company personnel to cut, reroute, or divert telephone lines for the purpose of preventing telephone communications between the suspect and any person other than a law enforcement officer or the law enforcement officer's designee, if such cutting, rerouting, or diverting of telephone lines is technically feasible and can be performed without endangering the lives of telephone company or other utility personnel.

(2) The good faith reliance by a telephone company on an oral or written order to cut, reroute, or divert telephone lines given by a supervising law enforcement officer under subsection (1) constitutes a complete defense to any civil, criminal, or administrative action arising out of such an order.

History.—ss. 1, 2, ch. 87-357; s. 1585, ch. 97-102.

934.21 Unlawful access to stored communications; penalties.—

(1) Except as provided in subsection (3), whoever:

- (a) Intentionally accesses without authorization a facility through which an electronic communication service is provided, or
- (b) Intentionally exceeds an authorization to access such facility,

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (2).

(2) The punishment for an offense under subsection (1) is as follows:

(a) If the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, the person is:

1. In the case of a first offense under this subsection, guilty of a misdemeanor of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 934.41.

2. In the case of any subsequent offense under this subsection, guilty of a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, s. 775.084, or s. 934.41.

(b) In any other case, the person is guilty of a misdemeanor of the second degree, punishable as provided in s. 775.082 or s. 775.083.

(3) Subsection (1) does not apply with respect to conduct authorized:

(a) By the person or entity providing a wire or electronic communications service;

(b) By a user of a wire or electronic communications service with respect to a communication of or intended for that user; or

(c) In s. 934.09, s. 934.23, or s. 934.24.

History.—s. 9, ch. 88-184; s. 9, ch. 89-269.

934.215 Unlawful use of a two-way communications device.—Any person who uses a two-way communications device, including, but not limited to, a portable two-way wireless communications device, to facilitate or further the commission of any felony offense commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

History.—s. 1, ch. 2001-114.

934.22 Voluntary disclosure of customer communications or records.—

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

(a) A provider of 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 remote computing service to the public may not knowingly divulge to:

1. Any person or entity the contents of any communication that is carried or maintained on that 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 remote computing service; and

b. 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) 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:

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

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).

History.—s. 9, ch. 88-184; s. 7, ch. 2002-72.

934.23 Required disclosure of customer communications or records.—

(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 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. As used in this section, the term “a court of competent jurisdiction” means a court that has jurisdiction over the investigation or that is otherwise authorized by law. An investigative or law enforcement officer may require the disclosure by a provider of electronic communication services of the contents of a wire or 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 a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service, not including the contents of a communication, 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);
3. Has the consent of the subscriber or customer to such disclosure; or
4. Seeks information under paragraph (b).

(b) 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 a subscriber to or customer of such service 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) 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.

History.—s. 9, ch. 88-184; s. 10, ch. 89-269; s. 13, ch. 2000-369; s. 8, ch. 2002-72; s. 2, ch. 2003-71.

934.24 Backup preservation; customer notification; challenges by customer.—

(1) An investigative or law enforcement officer acting under s. 934.23(2)(b) may include in the subpoena or court order upon which such action is based a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider must create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the investigative or law enforcement officer that such backup copy has been made. Such backup copy must be created within 2 business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer must be made by the investigative or law enforcement officer within 3 days after the receipt of such confirmation, unless such notice is delayed pursuant to s. 934.25(1).

(3) The service provider may not destroy the backup copy until the later of:

(a) The actual receipt by the requesting investigative or law enforcement officer of the information; or

(b) The resolution of any proceeding, including appeals thereof, concerning the government's subpoena or court order.

(4) The service provider shall release the backup copy to the requesting investigative or law enforcement officer no sooner than 14 days after the investigative or law enforcement officer's notice to the subscriber or

customer if such service provider:

(a) Has not received notice from the subscriber or customer that the subscriber or customer has challenged the investigative or law enforcement officer's request, and

(b) Has not initiated proceedings to challenge the request of the investigative or law enforcement officer.

(5) An investigative or law enforcement officer may seek to require the creation of a backup copy under subsection (1) if in the sole discretion of such officer there is reason to believe that notification under s. 934.23 of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or the service provider.

(6) Within 14 days after notice by the investigative or law enforcement officer to the subscriber or customer under subsection (2), the subscriber or customer may file a motion to quash the subpoena or vacate the court order seeking contents of electronic communications, with copies served upon the investigative or law enforcement officer and with written notice of such challenge to the service provider. A motion to vacate a court order must be filed in the court which issued the order. A motion to quash a subpoena must be filed in the circuit court in the circuit from which the subpoena issued. Such motion or application must contain an affidavit or sworn statement:

(a) Stating that the applicant is a subscriber or customer of the service from which the contents of electronic communications maintained for her or him have been sought, and

(b) Stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of ss. 934.21-934.28 in some other respect.

(7) Except as otherwise obtained under paragraph (3)(a), service must be made under this section upon an investigative or law enforcement officer by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the subscriber or customer has received pursuant to ss. 934.21-934.28. For the purposes of this subsection, the term "delivering" shall be construed in accordance with the definition of "delivery" as provided in Rule 1.080, Florida Rules of Civil Procedure.

(8) If the court finds that the customer has complied with subsections (6) and (7), the court shall order the investigative or law enforcement officer's agency or employing entity to file a sworn response, which may be filed in camera if the investigative or law enforcement officer's agency or employing entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings must be completed and the motion or application decided as soon as practicable after the filing of the investigative or law enforcement officer's agency's or employing entity's response.

(9)(a) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced.

(b) If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(10) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal or petition or request for discretionary review may be taken therefrom by the customer.

History.—s. 9, ch. 88-184; s. 1586, ch. 97-102.

934.25 Delayed notice.—

(1) An investigative or law enforcement officer acting under s. 934.23(2) may:

(a) Where a court order is sought, include in the application a request for an order delaying the notification required under s. 934.23(2) for a period not to exceed 90 days, which request the court shall grant if it determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in subsection (2).

(b) Where a subpoena is obtained, delay the notification required under s. 934.23(2) for a period not to exceed 90 days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in subsection (2).

(2) Any of the following acts constitute an adverse result for purposes of subsection (1):

(a) Endangering the life or physical safety of an individual.

(b) Fleeing from prosecution.

(c) Destroying or tampering with evidence.

(d) Intimidating potential witnesses.

(e) Seriously jeopardizing an investigation or unduly delaying a trial.

(3) The investigative or law enforcement officer shall maintain a true copy of a certification obtained under paragraph (1)(b).

(4) Extensions of the delay of notification provided in s. 934.23(2) of up to 90 days each may be granted by the court upon application, or by certification by an investigative or law enforcement officer, but only in accordance with subsection (6).

(5) Upon the expiration of the period of delay of notification under subsection (1) or subsection (4), the investigative or law enforcement officer must serve upon or deliver by registered or first-class mail to the subscriber or customer a copy of the process or request together with notice which:

(a) States with reasonable specificity the nature of the law enforcement inquiry, and

(b) Informs the subscriber or customer:

1. That information maintained for such subscriber or customer by the service provider named in the process or request was supplied to or requested by the investigative or law enforcement officer and the date on which such information was so supplied or requested.

2. That notification of such subscriber or customer was delayed.

3. What investigative or law enforcement officer or what court made the certification or determination pursuant to which that delay was made.

4. Which provision of ss. 934.21-934.28 allowed such delay.

(6) An investigative or law enforcement officer acting under s. 934.23, when not required to notify the subscriber or customer under s. 934.23(2)(a), or to the extent that such notice may be delayed pursuant to subsection (1), may apply to a court for an order commanding a provider of electronic communication service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of such warrant, subpoena, or court order. The court shall enter such order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in any of the following:

(a) Endangering the life or physical safety of an individual.

(b) Fleeing from prosecution.

(c) Destroying or tampering with evidence.

(d) Intimidating potential witnesses.

(e) Seriously jeopardizing an investigation or unduly delaying a trial.

(7) As used in paragraph (1)(b), the term "supervisory official" means the person in charge of an

investigating or law enforcement agency's or entity's headquarters or regional office; the state attorney of the circuit from which the subject subpoena has been issued; the statewide prosecutor; or an assistant state attorney or assistant statewide prosecutor specifically designated by the state attorney or statewide prosecutor to make such written certification.

(8) As used in subsection (5), the term "deliver" shall be construed in accordance with the definition of "delivery" as provided in Rule 1.080, Florida Rules of Civil Procedure.

History.—s. 9, ch. 88-184.

934.26 Cost reimbursement.—

(1) Except as otherwise provided in subsection (3), a governmental entity which obtains the contents of communications, records, or other information under s. 934.22, s. 934.23, or s. 934.24 shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs include any costs incurred due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(2) The amount of the fee provided by subsection (1) shall be as mutually agreed upon by the governmental entity and the person or entity providing the information or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information or the court before which a criminal prosecution relating to such information would be brought if no court order was issued for production of the information.

(3) The requirement of subsection (1) does not apply with respect to records or other information maintained by a communications carrier that relate to telephone toll records and telephone listings obtained under s. 934.23. The court may, however, order a payment as described in subsection (1) if the court determines the information required is unusually voluminous in nature or otherwise causes an undue burden on the provider.

History.—s. 9, ch. 88-184.

934.27 Civil action: relief; damages; defenses.—

(1) Except as provided in s. 934.23(5), any provider of electronic communication service, or subscriber or customer thereof, aggrieved by any violation of ss. 934.21-934.28 in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as is appropriate.

(2) In a civil action under this section, appropriate relief includes:

- (a) Such preliminary and other equitable or declaratory relief as is appropriate.
- (b) Damages under subsection (3).
- (c) A reasonable attorney's fee and other litigation costs reasonably incurred.

(3) The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a plaintiff entitled to recover be awarded less than \$1,000.

(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, including, but not limited to, a request of an investigative or law enforcement officer to 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.

(5) A civil action under this section may not be commenced later than 2 years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

History.—s. 9, ch. 88-184; s. 11, ch. 89-269; s. 14, ch. 2000-369; s. 9, ch. 2002-72.

934.28 Exclusivity of remedies and sanctions.—The remedies and sanctions described in ss. 934.21-934.27 are the only judicial remedies and sanctions for violation of those sections.

History.—s. 9, ch. 88-184.

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

(1) Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under s. 934.33.

(2) The prohibition of subsection (1) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service:

(a) Which relates to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of the provider or to the protection of users of that service from abuse of service or unlawful use of service;

(b) To record the fact that a wire or electronic communication was initiated or completed in order to protect the provider thereof, another provider furnishing service toward the completion of the wire communication, or a user of the service, from fraudulent, unlawful, or abusive use of service; or

(c) Where the consent of the user of the service has been obtained.

(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.

(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; 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.

(5) Whoever knowingly violates subsection (1) is guilty of a misdemeanor of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 934.41.

History.—s. 10, ch. 88-184; s. 12, ch. 89-269; s. 15, ch. 2000-369; s. 10, ch. 2002-72.

934.32 Application for an order for a pen register or a trap and trace device.—

(1)(a) The Governor, the Attorney General, a state attorney, the statewide prosecutor, or a designated assistant state attorney or assistant statewide prosecutor may make application for an order or an extension of an order under s. 934.33 authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to the judge of a court of competent jurisdiction.

(b) An investigative or law enforcement officer may make application for an order or an extension of an order under s. 934.33 authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to the judge of a court of competent jurisdiction.

(2) An application under subsection (1) must include:

(a) The identity of the applicant specified in the section and the identity of the law enforcement agency conducting the investigation, and

(b) A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the investigating agency.

History.—s. 10, ch. 88-184.

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 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 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 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.

History.—s. 10, ch. 88-184; s. 13, ch. 89-269; s. 11, ch. 2002-72.

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

(1) Upon the request of the applicant specified in s. 934.32(1), a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer or other applicant forthwith all information, facilities, and technical assistance necessary to accomplish the installation of a pen register 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, or such other assistance to support the investigation, if such assistance is directed by a court order as provided in s. 934.33(2)(b).

(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.

(3) A provider of a wire or electronic communication service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

(4) No cause of action shall lie in any court against any provider of a 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 under ss. 934.31-934.34.

(5) A good faith reliance on a court order or a statutory authorization is a complete defense against any civil or criminal action brought under ss. 934.31-934.34.

History.—s. 10, ch. 88-184; s. 14, ch. 89-269; s. 16, ch. 2000-369; s. 12, ch. 2002-72.

934.41 Alternative penalty.—

(1) In lieu of a fine otherwise authorized by law, any person convicted of engaging in conduct in violation of this chapter, through which she or he derived pecuniary value, or by which she or he caused property damage or other loss, may be sentenced to pay a fine that does not exceed three times the gross value gained or three times the gross loss caused, whichever is the greater, plus court costs and the costs of investigation and prosecution, reasonably incurred.

(2) The court shall hold a hearing to determine the amount of the fine authorized by subsection (1).

(3) For the purposes of subsection (1), “pecuniary value” means:

(a) Anything of value in the form of money, a negotiable instrument, or a commercial interest or anything else the primary significance of which is economic advantage; or

(b) Any other property or service that has a value in excess of \$100.

History.—s. 15, ch. 89-269; s. 1587, ch. 97-102.

934.42 Mobile tracking device authorization.—

(1) An investigative or law enforcement officer may make application to a judge of competent jurisdiction for an order authorizing or approving the installation and use of a mobile tracking device.

(2) An application under subsection (1) of this section must include:

(a) A statement of the identity of the applicant and the identity of the law enforcement agency conducting the investigation.

(b) A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the investigating agency.

(c) A statement of the offense to which the information likely to be obtained relates.

(d) A statement whether it may be necessary to use and monitor the mobile tracking device outside the jurisdiction of the court from which authorization is being sought.

(3) Upon application made as provided under subsection (2), the court, if it finds that the certification and statements required by subsection (2) have been made in the application, shall enter an ex parte order authorizing the installation and use of a mobile tracking device. Such order may authorize the use of the device within the jurisdiction of the court and outside that jurisdiction but within the State of Florida if the device is installed within the jurisdiction of the court.

(4) A court may not require greater specificity or additional information beyond that which is required by this section as a requisite for issuing an order.

(5) The standards established by the United States Supreme Court for the installation and monitoring of mobile tracking devices shall apply to the installation and use of any device as authorized by this section.

(6) As used in this section, a “tracking device” means an electronic or mechanical device which permits the tracking of the movement of a person or object.

History.—s. 16, ch. 89-269.

934.43 Criminal disclosure of subpoena, order, or authorization.—

(1) Any person having knowledge of a warrant, subpoena, application, order, or other authorization which has been issued or obtained pursuant to the action of an investigative or law enforcement officer as authorized by this chapter, who:

(a) With intent to obstruct, impede, or prevent an investigation, criminal prosecution, or civil, regulatory, or forfeiture action on behalf of the State of Florida or a political subdivision thereof; or

(b) With intent to obstruct, impede, or prevent the obtaining by an investigative or law enforcement officer of the information or materials sought pursuant to such warrant, subpoena, application, order, or authorization

gives notice or attempts to give notice of the investigation, criminal prosecution, or civil, regulatory, or forfeiture action, warrant, subpoena, application, order, or other authorization to any person commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, s. 775.084, or s. 934.41.

(2) This section does not prevent disclosure of the existence of the warrant, subpoena, application, order, or other authorization as otherwise provided under this chapter.

History.—s. 17, ch. 89-269.