

1 A bill to be entitled
2 An act relating to the interception of
3 communications; amending s. 934.02, F.S.;
4 revising definitions; including wire
5 communications within the meaning of an
6 electronic communications system; redefining
7 the terms "pen register" and "trap and trace
8 device"; defining the terms "foreign
9 intelligence information," "protected
10 computer," and "computer trespasser"; amending
11 s. 934.03, F.S.; authorizing the interception
12 of certain wire or electronic communications of
13 a computer trespasser; amending s. 934.07,
14 F.S.; authorizing the Department of Law
15 Enforcement to intercept wire, oral, or
16 electronic communications for purposes of
17 investigating certain additional offenses
18 concerning terrorism and the attempted or
19 threatened use of a destructive device or
20 weapon of mass destruction; requiring a law
21 enforcement agency to notify the Department of
22 Law Enforcement if an intercepted communication
23 provides evidence of certain acts of terrorism;
24 amending s. 934.09, F.S.; providing for the
25 interception of communications upon certain
26 findings of activities that threaten the
27 security of the nation or state; specifying
28 circumstances under which the court may
29 authorize the interception of communications
30 outside the court's jurisdiction; amending s.
31 934.08, F.S.; authorizing the disclosure of the

1 contents of an intercepted communication to
2 certain state and federal officials; amending
3 s. 934.22, F.S.; prohibiting a provider of
4 electronic communication service or a provider
5 of remote computing service from disclosing the
6 contents of communications or information
7 pertaining to a subscriber or customer;
8 specifying certain exceptions; amending s.
9 934.23, F.S.; providing for disclosure of
10 information pertaining to a subscriber or
11 customer under specified circumstances and
12 pursuant to a warrant; amending s. 934.27,
13 F.S.; providing that a request of an
14 investigative or law enforcement officer to
15 preserve records is a defense with respect to a
16 civil or criminal action concerning unlawful
17 access to communications; amending s. 934.31,
18 F.S.; prohibiting the recording of the contents
19 of communications by the use of a pen register
20 or trap and trace device; amending s. 934.33,
21 F.S.; requiring that a certification of an
22 order for a pen register or a trap and trace
23 device be provided to any person or entity not
24 specifically named in the order; requiring that
25 the order include information concerning
26 location of the device and geographic limits of
27 the order; requiring an investigative or law
28 enforcement agency to maintain a record of the
29 use of a pen register or trap and trace device
30 installed pursuant to an ex parte order;
31 requiring that the record be provided to the

1 court; amending s. 934.34, F.S.; providing for
2 a trap and trace device to be installed on
3 other facilities; providing an effective date.
4

5 Be It Enacted by the Legislature of the State of Florida:
6

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

11 934.02 Definitions.--As used in this chapter:

12 (1) "Wire communication" means any aural transfer made
13 in whole or in part through the use of facilities for the
14 transmission of communications by the aid of wire, cable, or
15 other like connection between the point of origin and the
16 point of reception including the use of such connection in a
17 switching station furnished or operated by any person engaged
18 in providing or operating such facilities for the transmission
19 of intrastate, interstate, or foreign communications or
20 communications affecting intrastate, interstate, or foreign
21 commerce. ~~Such term includes any electronic storage of such~~
22 ~~communication.~~

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

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

1 electronic equipment for the electronic storage of such
2 communications.

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

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

26 (24) "Foreign intelligence information" means
27 information, whether or not concerning a United States person,
28 as that term is defined in 50 U.S.C. s. 1801, which relates
29 to:
30
31

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

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

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

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

13 (25) "Protected computer" means:

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

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

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

24 (26) "Computer trespasser" means a person who accesses
25 a protected computer without authorization and thus does not
26 have a reasonable expectation of privacy with respect to any
27 communication transmitted to, through, or from the protected
28 computer. The term does not include a person known by the
29 owner or operator of the protected computer to have an
30 existing contractual relationship with the owner or operator
31

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

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

5 934.03 Interception and disclosure of wire, oral, or
6 electronic communications prohibited.--

7 (2)

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

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

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

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

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

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

27 934.07 Authorization for interception of wire, oral,
28 or electronic communications.--

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

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

4 (a) The Department of Law Enforcement or any law
5 enforcement agency as defined in s. 934.02 having
6 responsibility for the investigation of the offense as to
7 which the application is made when such interception may
8 provide or has provided evidence of the commission of the
9 offense of murder, kidnapping, aircraft piracy, arson,
10 gambling, robbery, burglary, theft, dealing in stolen
11 property, criminal usury, bribery, or extortion; any felony
12 violation of ss. 790.161-790.166, inclusive; any violation of
13 chapter 893; any violation of the provisions of the Florida
14 Anti-Fencing Act; any violation of chapter 895; any violation
15 of chapter 896; any violation of chapter 815; any violation of
16 chapter 847; any violation of s. 827.071; any violation of s.
17 944.40; or any conspiracy or solicitation to commit any
18 violation of the laws of this state relating to the crimes
19 specifically enumerated in this paragraph.

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

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

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

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

31

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

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

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

8 2. Involves a violation of s. 815.06; and

9 (b) Is intended to:

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

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

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

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

21 934.09 Procedure for interception of wire, oral, or
22 electronic communications.--

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

28 (a) An emergency exists that:

29 1. Involves immediate danger of death or serious
30 physical injury to any person, ~~or~~ the danger of escape of a
31

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

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

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

8
9 may intercept such wire, oral, or electronic communication if
10 an application for an order approving the interception is made
11 in accordance with this section within 48 hours after the
12 interception has occurred or begins to occur. In the absence
13 of an order, such interception shall immediately terminate
14 when the communication sought is obtained or when the
15 application for the order is denied, whichever is earlier. If
16 such application for approval is denied, or in any other case
17 in which the interception is terminated without an order
18 having been issued, the contents of any wire, oral, or
19 electronic communication intercepted shall be treated as
20 having been obtained in violation of s. 934.03(4), and an
21 inventory shall be served as provided for in paragraph (8)(e)
22 on the person named in the application.

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

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

29 1. The application is by an agent or officer of a law
30 enforcement agency and is approved by the Governor, the

31

1 Attorney General, the statewide prosecutor, or a state
2 attorney.

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

11 3. The judge finds that such showing has been
12 adequately made.

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

18
19 Consistent with this paragraph, a judge of competent
20 jurisdiction and limited to investigations of acts of
21 terrorism, as that term is defined in s. 934.07, the court may
22 authorize continued interception within this state, whether
23 the interception is both within or and outside the court's its
24 jurisdiction, if the application for the interception makes a
25 showing that some activity or conspiracy believed to be
26 related to, or in furtherance of, the criminal predicate for
27 the requested interception has occurred or will likely occur,
28 or the communication to be intercepted or expected to be
29 intercepted is occurring or will likely occur, in whole or in
30 part, within the jurisdiction of the court where the order is
31

1 being sought ~~original interception occurred within its~~
2 ~~jurisdiction.~~

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

7 934.09 Procedure for interception of wire, oral, or
8 electronic communications.--

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

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

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

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

27 3. The judge finds that such showing has been
28 adequately made.

29 4. The order authorizing or approving the interception
30 is limited to interception only for such time as it is
31 reasonable to presume that the person identified in the

1 application is or was reasonably proximate to the instrument
2 through which such communication will be or was transmitted.

3
4 Consistent with this paragraph, a judge of competent
5 jurisdiction may authorize interception within this state,
6 whether the interception is within or outside the court's
7 jurisdiction, if the application for the interception makes a
8 showing that some activity or conspiracy believed to be
9 related to, or in furtherance of, the criminal predicate for
10 the requested interception has occurred or will likely occur,
11 or the communication to be intercepted or expected to be
12 intercepted is occurring or will likely occur, in whole or in
13 part, within the jurisdiction of the court where the order is
14 being sought.

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

17 934.08 Authorization for disclosure and use of
18 intercepted wire, oral, or electronic communications.--

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

24 (a) The Department of Legal Affairs for use in
25 investigations or proceedings pursuant to s. 812.035, part II
26 of chapter 501, chapter 542, or chapter 895, to any attorney
27 authorized by law to investigate and institute any action on
28 behalf of the State of Florida or political subdivision
29 thereof, or to another investigative or law enforcement
30 officer to the extent that such disclosure is appropriate to
31

1 the proper performance of the official duties of the officer
2 or person making or receiving the disclosure.

3 (b) Any state or federal law enforcement official,
4 state or federal intelligence official, state or federal
5 protective services official, federal immigration official,
6 state or federal defense official, or state or federal
7 security official to the extent that the contents or evidence
8 includes foreign intelligence or counterintelligence, as
9 defined in 50 U.S.C. s. 401a, or foreign intelligence
10 information, as defined in this chapter, in order to assist
11 the official who receives that information in performing his
12 or her official duties. Any state or federal official who
13 receives information under this subsection may use that
14 information only as necessary in conducting official duties
15 and is subject to any limitations on the unauthorized
16 disclosure of such information.

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

19 934.22 Voluntary disclosure of customer communications
20 or records ~~contents~~.--

21 (1) Except as provided in subsection (2) or subsection
22 (3):

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

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

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

31

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

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

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

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

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

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

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

25 (b) As otherwise authorized in s. 934.03(2)(a), s.
26 934.07, or s. 934.23.

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

30
31

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

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

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

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

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

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

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

19 1. As is otherwise authorized in s. 934.23.

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

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

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

29 5. To any person other than a governmental entity.
30
31

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

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

6 934.23 Required disclosure of customer communications
7 or records ~~Requirements for governmental access.--~~

8 (1) An investigative or law enforcement officer may
9 require the disclosure by a provider of electronic
10 communication service of the contents of a wire or an
11 electronic communication that has been in electronic storage
12 in an electronic communications system for 180 days or less
13 only pursuant to a warrant issued by the judge of a court of
14 competent jurisdiction. An investigative or law enforcement
15 officer may require the disclosure by a provider of electronic
16 communication services of the contents of a wire or an
17 electronic communication that has been in electronic storage
18 in an electronic communications system for more than 180 days
19 by the means available under subsection (2).

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

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

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

- 1 1. Uses a subpoena; or
2 2. Obtains a court order for such disclosure under
3 subsection (5).

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

7 (a) On behalf of a subscriber or customer of such
8 service and received by means of electronic transmission from,
9 or created by means of computer processing of communications
10 received by means of electronic transmission from, a
11 subscriber or customer of such service.

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

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

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

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

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

5 3. Has the consent of the subscriber or customer to
6 such disclosure; or-

7 4. Seeks information under paragraph (b).

8 **(b)(c)** A provider of electronic communication service
9 or remote computing service shall disclose to an investigative
10 or law enforcement officer the name; address; local and long
11 distance telephone connection records, or records of session
12 times or durations; length of service, including the starting
13 date of service; types of services used; telephone or
14 instrument number or other subscriber number or identity,
15 including any temporarily assigned network address; and means
16 and source of payment, including any credit card or bank
17 account number of, ~~telephone toll billing records, telephone~~
18 number or other subscriber number or identity, and length of
19 service as a subscriber to or customer of such service and the
20 types of services the subscriber or customer used when the
21 governmental entity uses a subpoena or obtains such
22 information in the manner specified in paragraph (a) for
23 obtaining information under that paragraph.

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

27 (5) A court order for disclosure under subsection (2),
28 subsection (3), or subsection (4) shall issue only if the
29 investigative or law enforcement officer offers specific and
30 articulable facts showing that there are reasonable grounds to
31 believe the contents of a wire or electronic communication or

1 the records of other information sought are relevant and
2 material to an ongoing criminal investigation. A court
3 issuing an order pursuant to this section, on a motion made
4 promptly by the service provider, may quash or modify such
5 order if the information or records requested are unusually
6 voluminous in nature or compliance with such order otherwise
7 would cause an undue burden on such provider.

8 (6) No cause of action shall lie in any court against
9 any provider of wire or electronic communication service, its
10 officers, employees, agents, or other specified persons for
11 providing information, facilities, or assistance in accordance
12 with the terms of a court order, warrant, subpoena, or
13 certification under ss. 934.21-934.28.

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

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

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

31

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

3 934.27 Civil action: relief; damages; defenses.--

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

7 (a) A court warrant or order, a subpoena, or a
8 statutory authorization, including, but not limited to, a
9 request of an investigative or law enforcement officer to
10 preserve records or other evidence, as provided in s.
11 934.23(7).

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

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

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

18 934.31 General prohibition on pen register and trap
19 and trace device use; exception.--

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

29 (4)(a) Notwithstanding any other provision of this
30 chapter, any investigative or law enforcement officer
31 specially designated by the Governor, the Attorney General,

1 the statewide prosecutor, or a state attorney acting pursuant
2 to this chapter, who reasonably determines that:

3 1. An emergency exists which:

4 a. Involves immediate danger of death or serious
5 physical injury to any person or the danger of escape of a
6 prisoner; and

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

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

13
14 may have installed and use a pen register or trap and trace
15 device if, within 48 hours after the installation has occurred
16 or begins to occur, an order approving the installation or use
17 is issued in accordance with s. 934.33.

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

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

28 (d) A provider of wire or electronic service,
29 landlord, custodian, or other person who has furnished
30 facilities or technical assistance pursuant to this subsection
31 shall be held harmless from any claims and civil liability

1 resulting from the disclosure of information pursuant to this
2 subsection and shall be reasonably compensated for reasonable
3 expenses incurred in providing such facilities and assistance.

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

6 934.33 Issuance of an order for a pen register or a
7 trap and trace device.--

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

21 (2) An order issued under this section:

22 (a) Must specify the following:

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

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

29 3. The attributes of the communications to which the
30 order applies, including the number or other identifier and,
31 if known, the ~~physical~~ location of the telephone line or other

1 facility to which the pen register or trap and trace device is
2 to be attached or applied and, in the case of an order
3 authorizing installation and use of a trap and trace device,
4 the geographic limits of the ~~trap and trace~~ order.

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

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

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

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

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

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

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

1 (5) A court may not require greater specificity or
2 additional information beyond that which is required under s.
3 934.32 and this section as a requisite for issuing an order as
4 provided in this section.

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

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

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

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

21 4. Any information that was collected by the device.

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

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

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

3 934.34 Assistance in installation and use of a pen
4 register or a trap and trace device.--

5 (2) Upon the request of the applicant specified in s.
6 934.32(1), a provider of a wire or electronic communication
7 service, landlord, custodian, or other person shall install a
8 trap and trace device forthwith on the appropriate line or
9 other facility and shall furnish such investigative or law
10 enforcement officer or other applicant all additional
11 information, facilities, and technical assistance, including
12 installation and operation of the device unobtrusively and
13 with a minimum of interference with the services that the
14 person so ordered by the court accords the party with respect
15 to whom the installation and use is to take place if such
16 installation and assistance is directed by a court order as
17 provided in s. 934.33(2)(b). Unless otherwise ordered by the
18 court, the results of the trap and trace device shall be
19 furnished, pursuant to s. 934.31(4) or s. 934.33(2)(b), to an
20 officer of the law enforcement agency designated in the court
21 order at reasonable intervals during regular business hours
22 for the duration of the order. The obligation of a provider of
23 electronic communication service under such an order or under
24 such emergency pen register or trap and trace device
25 installation may include, but is not limited to, conducting an
26 in-progress trace, or providing other assistance to support
27 the investigation as may be specified in the order.

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