

By Senator Smith

5-1350A-02

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
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 that 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 in whole or in part, within the jurisdiction of the court
29 where the order is being sought original interception occurred
30 within its jurisdiction.

31

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

5 934.09 Procedure for interception of wire, oral, or
6 electronic communications.--

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

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

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

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

25 3. The judge finds that such showing has been
26 adequately made.

27 4. The order authorizing or approving the interception
28 is limited to interception only for such time as it is
29 reasonable to presume that the person identified in the
30 application is or was reasonably proximate to the instrument
31 through which such communication will be or was transmitted.

1
2 Consistent with this paragraph, a judge of competent
3 jurisdiction may authorize interception within this state,
4 whether the interception is within or outside the court's
5 jurisdiction, if the application for the interception makes a
6 showing that some activity or conspiracy believed to be
7 related to, or in furtherance of, the criminal predicate for
8 the requested interception has occurred or will likely occur,
9 in whole or in part, within the jurisdiction of the court
10 where the order is being sought.

11 Section 6. Subsection (6) is added to section 934.08,
12 Florida Statutes, to read:

13 934.08 Authorization for disclosure and use of
14 intercepted wire, oral, or electronic communications.--

15 (6) Any investigative or law enforcement officer who,
16 by any means authorized by this chapter, obtains knowledge of
17 the contents of any wire, oral, or electronic communication or
18 evidence derived from the contents of any wire, oral, or
19 electronic communication may disclose the contents or evidence
20 to any state or federal law enforcement official, state or
21 federal intelligence official, state or federal protective
22 services official, federal immigration official, state or
23 federal defense official, or state or federal security
24 official to the extent that the contents or evidence includes
25 foreign intelligence or counterintelligence, as defined in 50
26 U.S.C. s. 401a, or foreign intelligence information, as
27 defined in this chapter, in order to assist the official who
28 receives that information in performing his or her official
29 duties. Any state or federal official who receives information
30 under this subsection may use that information only as
31 necessary in conducting official duties and is subject to any

1 limitations on the unauthorized disclosure of such
2 information.

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

5 934.22 Voluntary disclosure of customer communications
6 or records contents.--

7 (1) Except as provided in subsection (2) or subsection
8 (3):

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

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

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

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

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

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

28 b.2. ~~Solely for the purpose of providing storage or~~
29 ~~computer processing services to its subscriber or customer, if~~
30 ~~the provider is not authorized to access the contents of any~~
31

1 such communication for purposes of providing any service other
2 than storage or computer processing; ~~or-~~

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

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

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

11 (b) As otherwise authorized in s. 934.03(2)(a), s.
12 934.07, or s. 934.23.

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

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

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

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

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

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

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

31

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

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

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

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

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

14 5. To any person other than a governmental entity.

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

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

20 934.23 Required disclosure of customer communications
21 or records ~~Requirements for governmental access.--~~

22 (1) An investigative or law enforcement officer may
23 require the disclosure by a provider of electronic
24 communication service of the contents of a wire or an
25 electronic communication that has been in electronic storage
26 in an electronic communications system for 180 days or less
27 only pursuant to a warrant issued by the judge of a court of
28 competent jurisdiction. An investigative or law enforcement
29 officer may require the disclosure by a provider of electronic
30 communication services of the contents of a wire or an
31 electronic communication that has been in electronic storage

1 in an electronic communications system for more than 180 days
2 by the means available under subsection (2).

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

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

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

15 1. Uses a subpoena; or

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

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

21 (a) On behalf of a subscriber or customer of such
22 service and received by means of electronic transmission from,
23 or created by means of computer processing of communications
24 received by means of electronic transmission from, a
25 subscriber or customer of such service.

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

31

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

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

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

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

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

22 4. Seeks information under paragraph (b).

23 ~~(b)(c)~~ A provider of electronic communication service
24 or remote computing service shall disclose to an investigative
25 or law enforcement officer the name; address; local and long
26 distance telephone connection records, or records of session
27 times or durations; length of service, including the starting
28 date of service; types of services used; telephone or
29 instrument number or other subscriber number or identity,
30 including any temporarily assigned network address; and means
31 and source of payment, including any credit card or bank

1 account number of, ~~telephone toll billing records, telephone~~
2 ~~number or other subscriber number or identity, and length of~~
3 ~~service as a subscriber to or customer of such service and the~~
4 ~~types of services the subscriber or customer used when the~~
5 governmental entity uses a subpoena or obtains such
6 information in the manner specified in paragraph (a) for
7 obtaining information under that paragraph.

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

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

23 (6) No cause of action shall lie in any court against
24 any provider of wire or electronic communication service, its
25 officers, employees, agents, or other specified persons for
26 providing information, facilities, or assistance in accordance
27 with the terms of a court order, warrant, subpoena, or
28 certification under ss. 934.21-934.28.

29 (7)(a) A provider of wire or electronic communication
30 services or a remote computing service, upon the request of an
31 investigative or law enforcement officer, shall take all

1 necessary steps to preserve records and other evidence in its
2 possession pending the issuance of a court order or other
3 process.

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

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

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

17 934.27 Civil action: relief; damages; defenses.--

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

21 (a) A court warrant or order, a subpoena, or a
22 statutory authorization, including, but not limited to, a
23 request of an investigative or law enforcement officer to
24 preserve records or other evidence, as provided in s.
25 934.23(7).

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

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

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

1 934.31 General prohibition on pen register and trap
2 and trace device use; exception.--

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

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

17 1. An emergency exists which:

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

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

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

28
29 may have installed and use a pen register or trap and trace
30 device if, within 48 hours after the installation has occurred
31

1 or begins to occur, an order approving the installation or use
2 is issued in accordance with s. 934.33.

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

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

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

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

22 934.33 Issuance of an order for a pen register or a
23 trap and trace device.--

24 (1) Upon application made under s. 934.32, the court
25 shall enter an ex parte order authorizing the installation and
26 use of a pen register or a trap and trace device within the
27 jurisdiction of the court if the court finds that the
28 applicant specified in s. 934.32(1) has certified to the court
29 that the information likely to be obtained by such
30 installation and use is relevant to an ongoing criminal
31 investigation. Whenever such order is served on any person or

1 entity not specifically named in the order, upon request of
2 such person or entity, the person specified in s. 934.32 who
3 has requested and is serving such order shall provide written
4 or electronic certification that such order applies to the
5 person or entity being served.

6 (2) An order issued under this section:

7 (a) Must specify the following:

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

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

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

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

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

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

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

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

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

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

21 (5) A court may not require greater specificity or
22 additional information beyond that which is required under s.
23 934.32 and this section as a requisite for issuing an order as
24 provided in this section.

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

31

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

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

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

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

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

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

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

24 934.34 Assistance in installation and use of a pen
25 register or a trap and trace device.--

26 (2) Upon the request of the applicant specified in s.
27 934.32(1), a provider of a wire or electronic communication
28 service, landlord, custodian, or other person shall install a
29 trap and trace device forthwith on the appropriate line or
30 other facility and shall furnish such investigative or law
31 enforcement officer or other applicant all additional

1 information, facilities, and technical assistance, including
2 installation and operation of the device unobtrusively and
3 with a minimum of interference with the services that the
4 person so ordered by the court accords the party with respect
5 to whom the installation and use is to take place if such
6 installation and assistance is directed by a court order as
7 provided in s. 934.33(2)(b). Unless otherwise ordered by the
8 court, the results of the trap and trace device shall be
9 furnished, pursuant to s. 934.31(4) or s. 934.33(2)(b), to an
10 officer of the law enforcement agency designated in the court
11 order at reasonable intervals during regular business hours
12 for the duration of the order. The obligation of a provider of
13 electronic communication service under such an order or under
14 such emergency pen register or trap and trace device
15 installation may include, but is not limited to, conducting an
16 in-progress trace, or providing other assistance to support
17 the investigation as may be specified in the order.

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

20
21
22
23
24
25
26
27
28
29
30
31

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

SENATE SUMMARY

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