SENATE STAFF ANALYSIS AND ECONOMIC IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

BILL: CS/SB 1774

SPONSOR: Criminal Justice Committee and Senator Smith

SUBJECT: Interception of Communications

DATE: February 25, 2002 REVISED: _____ _____ _____ _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Erickson	Cannon	CJ	Favorable/CS
2.			JU	
3.				
4.				
5.				
6.				

I. Summary:

Committee Substitute for Senate Bill 1774 amends ch. 934, F.S., which addresses interception of communications. Most of the changes in the CS create parallel state provisions to the provisions of federal law relating to interception of communications that were recently created or amended by the USA Patriot Act. Those changes are summarized as follows:

Amends the definitions section of ch. 934, F.S., to modify current definitions and create new ones consistent with the new or amended federal definitions.

Permits a state judge having felony jurisdiction to authorize initial and ongoing interception of communications anywhere in the state when the application for an 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 and the communications 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 sought.

Allows a person acting under color or law, in order to determine if any violations of law are taking place, to intercept communications of an entity that is trespassing in the "protected computer" of another person when so authorized by the owner/operator of the "protected computer."

Allows court-ordered interception in cases involving offenses involving bombs, destructive devices, and weapons of mass destruction.

Clarifies provisions relevant to interception in investigations of acts of terrorism. Only FDLE has the authority to conduct such interception. The amendments allow FDLE,

consistent with current law, to utilize resources to effectively investigate acts of terrorism, including the use of personnel from other agencies who would be acting at the direction of FDLE.

Provides a method by which FDLE is brought into a local agency's wire intercept investigation when it turns out that those being intercepted have turned to terrorism-related crimes.

Authorizes an emergency intercept when there is evidence that there are communications that involve conspiratorial activities threatening national or state security.

Eliminates sunsetting of "continued interception" provision and extends that provision beyond interceptions in investigations of acts of terrorism.

Permits an officer who legally obtains information under ch. 934, F.S., to share information about "foreign intelligence or counterintelligence."

Modifies provisions dealing with release of the contents of communications in the custody of a provider of a remote computing service or electronic communications service to the government and others. It provides for special emergency release to the government or others of a record or other information pertaining to a subscriber/customer of identified providers in an emergency involving immediate danger of death or serious physical injury.

Sets forth the type of legal process needed in order for an investigative or law enforcement officer to obtain certain records from a provider of electronic communication service or remote computing service. It sets forth a new and expanded listing of the types of records contemplated to be released upon receipt of the appropriate legal documents.

Provides a defense to civil liability in s. 934.27, F.S., to cases in which an officer requests that records be preserved in accordance with current law. This provision extends protections to the providers of services that can include individual citizens or companies.

Clarifies that an investigative or law enforcement officer shall use technology reasonably available to him or her which restricts the recording or decoding of electronic or other impulses to the dialing (now also adds routing, addressing) and signaling information used in the processing and transmitting of wire or electronic communication so as not to include the contents of any wire or electronic communications.

Requires an officer serving an order for a pen register or a trap and trace device, if requested, to provide the person or entity served with written or electronic certification that the order applies to that person or entity if they are not specifically named in the order.

Provides that installation and use of pen registers and trap and trace devices can relate to more than just telephones and may entail the application of the devices to the telephone

line or other facility rather than the attachment of the devices to the telephone lines or other facility.

Sets forth detailed provisions dealing with requirements needed when an investigative or law enforcement officer implements an ex parte order by installing and using his own pen register or trap and trace device on a packet-switched data network of an electronic communications service to the public.

This CS substantially amends the following sections of the Florida Statutes: 934.02; 934.03; 934.07; 934.08; 934.09; 934.22; 934.23; 934.27; 934.31; 934.33; and 934.34.

II. Present Situation:

A. WIRETAP PROVISIONS OF THE USA PATRIOT ACT

The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (the USA Patriot Act) Act of 2001" (H.R. 3162; PL 107-56, 107th Congress), contains numerous provisions amending federal laws addressing or relevant to interception of communications.

Section 201: Authority to Intercept Wire, Oral, and Electronic Communications Relating to Terrorism
Section 201 provides authority to intercept wire, oral, and electronic communications relating to terrorism by adding criminal violations relating to terrorism (such as offenses relating to weapons of mass destruction) to the list of predicate statutes in the criminal procedures for interception of communications under Chapter 119 of Title 18, United States Code.

Section 202: Authority to Intercept Voice Communications in Computer Hacking Investigations
Section 202 "amends 18 U.S.C. 2516(1) – the subsection that lists those crimes for which investigators may obtain a wiretap order for wire communications – by adding felony violations of 18 U.S.C. 1030 to the list of predicate offenses." *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, Computer Crime and Intellectual Property Section, U.S. Department of Justice.

"Under previous law, investigators could not obtain a wiretap order to intercept wire communications (those involving the human voice) for violations of the Computer Fraud and Abuse Act (18 U.S.C. 1030). For example, in several investigations, hackers have stolen teleconferencing services from a telephone company and used this mode of communication to plan and execute hacking attacks." *Id.*

Section 203:
Section 203 "[a]mends rule 6 of the Federal Rules of Criminal Procedure (FRCrP) to permit the sharing of grand jury information that involves foreign intelligence or counterintelligence with Federal law enforcement, intelligence, protective, immigration, national defense, or national security officials . . ., subject to specified requirements." Congressional Research Service summary.

This section also "[a]uthorizes an investigative or law enforcement officer, or an attorney for the Government, who, by authorized means, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom to disclose such contents to such officials to the extent that such contents include foreign intelligence or counterintelligence." *Id.*

This section also "[d]irects the Attorney General to establish procedures for the disclosure of information (pursuant to the code and the FRCrP) that identifies a United States person, as defined in the Foreign Intelligence Surveillance Act of 1978 (FISA)." *Id.*

Section 209: Obtaining Voice-mail and Other Stored Voice Communications
Section 209 "alters the way in which the wiretap statute and ECPA [the Electronic Communications Privacy Act, 18 U.S.C. 2703 et seq.,] apply to stored voice communications. The amendments delete 'electronic storage' of wire communications from the definition of 'wire communication' in section 2510 and insert language in section 2703 to ensure that stored wire communications are covered under the same rules as stored electronic communications. Thus, law enforcement can now obtain such communications using the procedures set out in section 2703 (such as a search warrant), rather than those in the wiretap statute (such as a wiretap order)." *Field Guidance, supra.* (bracketed information provided by analyst)

"Under previous law, the [ECPA] governed law enforcement access to stored electronic communications (such as e-mail), but not stored wire communications (such as voice-mail). Instead, the wiretap statute governed such access because the definition of 'wire communication' (18 U.S.C. 2510(1)) included stored communications, arguably requiring law enforcement to use a wiretap order (rather than a search warrant) to obtain unopened voice communications. Thus, law enforcement authorities used a wiretap order to obtain voice communications stored with a third party provider but could use a search warrant if that same information were stored on an answering machine inside a criminal's home.

"Regulating stored wire communications through section 2510(1) created large and unnecessary burdens for criminal investigations. Stored voice communications possess few of the sensitivities associated with the real-time interception of telephones, making the extremely burdensome process of obtaining a wiretap order unreasonable.

"Moreover, in large part, the statutory framework envisions a world in which technology-mediated voice communications (such as telephone calls) are conceptually distinct from non-voice communications (such as faxes, pager messages, and e-mail). To the limited extent that Congress acknowledged that data and voice might co-exist in a single transaction, it did not anticipate the convergence of these two kinds of communications typical of today's telecommunications networks.

"With the advent of MIME — Multipurpose Internet Mail Extensions — and similar features, an e-mail may include one or more 'attachments' consisting of any type of data, including voice recordings. As a result, a law enforcement officer seeking to obtain a suspect's unopened e-mail from an ISP by means of a search warrant (as required under 18 U.S.C. 2703(a)) had no way of knowing whether the inbox messages include voice attachments (i.e., wire communications)

which could not be compelled using a search warrant." *Id.* (bracketed information provided by analyst)

Section 210: Scope of Subpoenas for Electronic Evidence
Section 210 amends 18 U.S.C. 2703(c) to "update and expand the narrow list of records that law enforcement authorities may obtain with a subpoena. The new subsection 2703(c)(2) includes 'records of session times and durations,' as well as 'any temporarily assigned network address.' In the Internet context, such records include the Internet Protocol (IP) address assigned by the provider to the customer or subscriber for a particular session, as well as the remote IP address from which a customer connects to the provider. Obtaining such records will make the process of identifying computer criminals and tracing their Internet communications faster and easier.

"Moreover, the amendments clarify that investigators may use a subpoena to obtain the 'means and source of payment' that a customer uses to pay for his or her account with a communications provider, 'including any credit card or bank account number.' 18 U.S.C. 2703(c)(2)(F). While generally helpful, this information will prove particularly valuable in identifying the users of Internet services where a company does not verify its users' biographical information." *Field Guidance*, *supra.*

"Subsection 2703(c) allows the government to use a subpoena to compel a limited class of information, such as the customer's name, address, length of service, and means of payment. Prior to the amendments in Section 210 of the Act, however, the list of records that investigators could obtain with a subpoena did not include certain records (such as credit card number or other form of payment for the communication service) relevant to determining a customer's true identity. In many cases, users register with Internet service providers using false names. In order to hold these individuals responsible for criminal acts committed online, the method of payment is an essential means of determining true identity.

"Moreover, many of the definitions in section 2703(c) were technology-specific, relating primarily to telephone communications. For example, the list included 'local and long distance telephone toll billing records,' but did not include parallel terms for communications on computer networks, such as 'records of session times and durations.' Similarly, the previous list allowed the government to use a subpoena to obtain the customer's 'telephone number or other subscriber number or identity,' but did not define what that phrase meant in the context of Internet communications." *Id.*

Section 212: Emergency Disclosures by Communications Providers
Section 212 "corrects . . . inadequacies in previous law. Section 212 amends subsection 2702(b)(6) to permit, but not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers.

"The amendments in Section 212 of the Act also change ECPA to allow providers to disclose information to protect their rights and property. It accomplishes this change by two related sets of amendments. First, amendments to sections 2702 and 2703 of title 18 simplify the treatment of voluntary disclosures by providers by moving all such provisions to 2702. Thus, section 2702

now regulates all permissive disclosures (of content and non-content records alike), while section 2703 covers only compulsory disclosures by providers. Second, an amendment to new subsection 2702(c)(3) clarifies that service providers do have the statutory authority to disclose non-content records to protect their rights and property." *Field Guidance, supra.*

"Previous law relating to voluntary disclosures by communication service providers was inadequate in two respects. First, it contained no special provision allowing providers to disclose customer records or communications in emergencies. If, for example, an Internet service provider ('ISP') independently learned that one of its customers was part of a conspiracy to commit an imminent terrorist attack, prompt disclosure of the account information to law enforcement could save lives. Since providing this information did not fall within one of the statutory exceptions, however, an ISP making such a disclosure could be sued civilly.

"Second, prior to the Act, the law did not expressly permit a provider to voluntarily disclose non-content records (such as a subscriber's login records) to law enforcement for purposes of self-protection, even though providers could disclose the content of communications for this reason. *See* 18 U.S.C. 2702(b)(5), 2703(c)(1)(B). Yet the right to disclose the content of communications necessarily implies the less intrusive ability to disclose non-content records. *Cf. United States v. Auler*, 539 F.2d 642, 646 n.9 (7th Cir. 1976) (phone company's authority to monitor and disclose conversations to protect against fraud necessarily implies right to commit lesser invasion of using, and disclosing fruits of, pen register device) (*citing United States v. Freeman*, 524 F.2d 337, 341 (7th Cir. 1975)). Moreover, as a practical matter, providers must have the right to disclose to law enforcement the facts surrounding attacks on their systems. For example, when an ISP's customer hacks into the ISP's network, gains complete control over an e-mail server, and reads or modifies the e-mail of other customers, the provider must have the legal ability to report the complete details of the crime to law enforcement." *Id.*

Section 216 makes numerous changes to the federal law relating to pen register and trap and trace devices. "The pen register and trap and trace statute (the 'pen/trap' statute) [18 U.S.C. 3121 et seq.] governs the prospective collection of non-content traffic information associated with communications, such as the phone numbers dialed by a particular telephone. Section 216 updates the pen/trap statute in three important ways: (1) the amendments clarify that law enforcement may use pen/trap orders to trace communications on the Internet and other computer networks; (2) pen/trap orders issued by federal courts now have nationwide effect; and (3) law enforcement authorities must file a special report with the court whenever they use a pen/trap order to install their own monitoring device (such as the FBI's DCS1000) on computers belonging to a public provider." *Id.* (bracketed information provided by analyst) Provided is a breakdown of the changes:

Using pen/trap orders to trace communications on computer networks

"Section 216 of the Act amends sections 3121, 3123, 3124, and 3127 of title 18 to clarify that the pen/trap statute applies to a broad variety of communications technologies. References to the target 'line,' for example, are revised to encompass a 'line or other facility.' Such a facility might include, for example, a cellular telephone number; a specific cellular telephone identified by its electronic serial number; an Internet user account or e-mail address; or an Internet Protocol address, port number, or similar computer network address or range of addresses. In addition, because the statute takes into account a wide variety of such facilities, amendments to section 3123(b)(1)(C) now allow applicants for pen/trap orders to submit a description of the communications to be traced using any of these or other identifiers.

"Moreover, the amendments clarify that orders for the installation of pen register and trap and trace devices may obtain any non-content information – all 'dialing, routing, addressing, and signaling information' – utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the 'To' and 'From' information contained in an e-mail header. Pen/trap orders cannot, however, authorize the interception of the content of a communication, such as words in the 'subject line' or the body of an e-mail.

"Further, because the pen register or trap and trace 'device' often cannot be physically 'attached' to the target facility, Section 216 makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the amended statute allows the pen register or trap and trace device to be 'attached or applied' to the target facility. Likewise, Section 216 revises the definitions of 'pen register' and 'trap and trace device' in section 3127 to include an intangible 'process' (such as a software routine) which collects the same information as a physical device." *Field Guidance, supra.*

"When Congress enacted the pen/trap statute in 1986, it could not anticipate the dramatic expansion in electronic communications that would occur in the following fifteen years. Thus, the statute contained certain language that appeared to apply to telephone communications and that did not unambiguously encompass communications over computer networks. Although numerous courts across the country have applied the pen/trap statue to communications on computer networks, no federal district or appellate court has explicitly ruled on its propriety. Moreover, certain private litigants have challenged the application of the pen/trap statute to such electronic communications based on the statute's telephone-specific language." *Id.*

Nationwide effect of pen/trap orders

"Section 216 of the Act divides section 3123 of title 18 into two separate provisions. New subsection (a)(1) gives federal courts the authority to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order.

"For example, a federal prosecutor may obtain an order to trace calls made to a telephone within the prosecutor's local district. The order applies not only to the local carrier serving that line, but also to other providers (such as long-distance carriers and regional carriers in other parts of the country) through whom calls are placed to the target telephone. In some circumstances, the investigators may have to serve the order on the first carrier in the chain and receive from that carrier information identifying the communication's path to convey to the next carrier in the chain. The investigator would then serve the same court order on the next carrier, including the additional relevant connection information learned from the first carrier; the second carrier would then provide the connection information in its possession for the communication. The investigator would repeat this process until the order has been served on the originating carrier who is able to identify the source of the communication.

"When prosecutors apply for a pen/trap order using this procedure, they generally will not know the name of the second or subsequent providers in the chain of communication covered by the order. Thus, the application and order will not necessarily name these providers. The amendments to section 3123 therefore specify that, if a provider requests it, law enforcement must provide a 'written or electronic certification' that the order applies to that provider.

"The amendments in Section 216 of the Act also empower courts to authorize the installation and use of pen/trap devices in other districts. Thus, for example, if a terrorism or other criminal investigation based in Virginia uncovers a conspirator using a phone or an Internet account in New York, the Virginia court can compel communications providers in New York to assist investigators in collecting information under a Virginia pen/trap order.

"Consistent with the change above, Section 216 of the Act modifies section 3123(b)(1)(C) of title 18 to eliminate the requirement that federal pen/trap orders specify their geographic limits. However, because the new law gives nationwide effect for federal pen/trap orders, an amendment to section 3127(2)(A) imposes a 'nexus' requirement: the issuing court must have jurisdiction over the particular crime under investigation." *Field Guidance, supra.*

"Under previous law, a court could only authorize the installation of a pen/trap device 'within the jurisdiction of the court.' Because of deregulation in the telecommunications industry, however, many providers may carry a single communication. For example, a telephone call may be carried by a competitive local exchange carrier, which passes it to a local Bell Operating Company, which passes it to a long distance carrier, which hands it to a local exchange carrier elsewhere in the U.S., which in turn may finally hand it to a cellular carrier. If these carriers do not pass source information with each call, identifying that source may require compelling information from a string of providers located throughout the country – each requiring a separate order.

"Moreover, since, under previous law, a court could only authorize the installation of a pen/trap device within its own jurisdiction, when one provider indicated that the source of a communication was a different carrier in another district, a second order in the new

district became necessary. This order had to be acquired by a supporting prosecutor in the new district from a local federal judge – neither of whom had any other interest in the case. Indeed, in one case investigators needed three separate orders to trace a hacker's communications. This duplicative process of obtaining a separate order for each link in the communications chain has delayed or — given the difficulty of real-time tracing — completely thwarted important investigations." *Id.*

Reports for use of law enforcement pen/trap devices on computer networks

"Section 216 of the Act also contains an additional requirement for the use of pen/trap devices in a narrow class of cases. Generally, when law enforcement serves a pen/trap order on a communication service provider that provides Internet access or other computing services to the public, the provider itself should be able to collect the needed information and provide it to law enforcement. In certain rare cases, however, the provider may be unable to carry out the court order, necessitating installation of a device (such as Etherpeek or the FBI's DCS1000) to collect the information. In these infrequent cases, the amendments in section 216 require the law enforcement agency to provide the following information to the court under seal within thirty days: (1) the identity of the officers who installed or accessed the device; (2) the date and time the device was installed, accessed, and uninstalled; (3) the configuration of the device at installation and any modifications to that configuration; and (4) the information collected by the device. 18 U.S.C. 3123(a)(3)." *Field Guidance, supra.*

Section 217: Intercepting the Communications of Computer Trespassers

Section 217 allows "victims of computer attacks to authorize persons 'acting under color of law' to monitor trespassers on their computer systems. Under new section 2511(2)(i), law enforcement may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before monitoring can occur, however, four requirements must be met. First, section 2511(2)(i)(I) requires that the owner or operator of the protected computer must authorize the interception of the trespasser's communications. Second, section 2511(2)(i)(II) requires that the person who intercepts the communication be lawfully engaged in an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation.

"Third, section 2511(2)(i)(III) requires that the person acting under color of law have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. Fourth, section 2511(2)(i)(IV) requires that investigators intercept only the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer.

"Finally, section 217 of the Act amends section 2510 of title 18 to create a definition of 'computer trespasser.' Such trespassers include any person who accesses a protected computer (as defined in section 1030 of title 18) without authorization. In addition, the definition explicitly excludes any person 'known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the

computer.' 18 U.S.C. 2510(21). For example, certain Internet service providers do not allow their customers to send bulk unsolicited e-mails (or 'spam'). Customers who send spam would be in violation of the provider's terms of service, but would not qualify as trespassers – both because they are authorized users and because they have an existing contractual relationship with the provider." *Field Guidance, supra.*

"Although the wiretap statute allows computer owners to monitor the activity on their machines to protect their rights and property, until Section 217 of the Act was enacted it was unclear whether computer owners could obtain the assistance of law enforcement in conducting such monitoring. This lack of clarity prevented law enforcement from assisting victims to take the natural and reasonable steps in their own defense that would be entirely legal in the physical world. In the physical world, burglary victims may invite the police into their homes to help them catch burglars in the act of committing their crimes. The wiretap statute should not block investigators from responding to similar requests in the computer context simply because the means of committing the burglary happen to fall within the definition of a 'wire or electronic communication' according to the wiretap statute. Indeed, because providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves, they commonly have no effective way to exercise their rights to protect themselves from unauthorized attackers. This anomaly in the law created, as one commentator has noted, a 'bizarre result,' in which a 'computer hacker's undeserved statutory privacy right trumps the legitimate privacy rights of the hacker's victims.' Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1300 (2000)." *Id.*

Section 220: Nationwide Search Warrants for E-mail

"Section 220 amends 18 U.S.C. 2703(a) to authorize courts with jurisdiction over the offense to issue search warrants for electronic communications in electronic storage anywhere in the United States, without requiring the intervention of their counterparts in the districts where Internet service providers are located. The effect of this provision is to limit forum shopping by limiting authorization for issuance of search warrants to those courts with jurisdiction over the offense." *Field Guidance, supra.*

"Section 2703(a) requires the government to use a search warrant to compel a provider to disclose unopened e-mail less than six months old. Because Rule 41 of the Federal Rules of Criminal Procedure requires that the 'property' to be obtained be 'within the district' of the issuing court, however, some courts have declined to issue section 2703(a) warrants for e-mail located in other districts. Unfortunately, this refusal has placed an enormous administrative burden on those districts in which major ISPs are located, such as the Eastern District of Virginia and the Northern District of California, even though these districts may have no relationship with the criminal acts under investigation. In addition, requiring investigators to obtain warrants in distant jurisdictions has slowed time-sensitive investigations." *Id.*

Section 814: Expanding the Definition of "Protected Computer" in Subsection 1030(e)(2) to Include Computers in Foreign Countries

"Section 814 of the Act amends the definition of 'protected computer' [in 18 U.S.C. 1030(e)(2)] to make clear that this term includes computers outside of the United States so long as they affect 'interstate or foreign commerce or communication of the United States.' 18 U.S.C. 1030(e)(2)(B). By clarifying the fact that a domestic offense exists, the United States can now

use speedier domestic procedures to join in international hacker investigations. As these crimes often involve investigators and victims in more than one country, fostering international law enforcement cooperation is essential." *Field Guidance, supra.* (bracketed information provided by analyst)

"Before the amendments in Section 814 of the Act, section 1030 of title 18 defined 'protected computer' as a computer used by the federal government or a financial institution, or one 'which is used in interstate or foreign commerce.' 18 U.S.C. 1030(e)(2). The definition did not explicitly include computers outside the United States.

"Because of the interdependency and availability of global computer networks, hackers from within the United States are increasingly targeting systems located entirely outside of this country. . . . In addition, individuals in foreign countries frequently route communications through the United States, even as they hack from one foreign country to another. In such cases, their hope may be that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution." *Id.*

Section 815: Additional Defense to Civil Actions Relating to Preserving Records in Response to Government Requests

"Section 815 added to an existing defense to a cause for damages for violations of the Electronic Communications Privacy Act, Chapter 121 of Title 18. Under prior law it was a defense to such a cause of action to rely in good faith on a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization. This amendment makes clear that the 'statutory authorization' defense includes good-faith reliance on a government request to preserve evidence under 18 U.S.C. 2703(f)." *Field Guidance, supra.*

Sunsetting of Provisions

Pursuant to Section 224 of the USA Patriot Act, the following sections of the Act (relevant to this analysis) will sunset on December 31, 2005, unless reenacted by Congress: 201; 202; 203(b); 209; 212; 217; and 220.

B. EMERGENCY INTERCEPT INVOLVING CONSPIRATORIAL ACTIVITIES THREATENING THE NATIONAL SECURITY INTEREST

Title 18 U.S.C. 2518(7) authorizes application for an intercept if the applicant reasonably believes an emergency exists that involves conspiratorial activities threatening the national security interest.

C. FLORIDA'S LAWS REGARDING INTERCEPTION OF COMMUNICATIONS

Provided is a summary from the General Counsel of the Florida Department of Law Enforcement (FDLE) of the Florida statutory requirements for interception of communications:

Florida law governing interception of communications and related topics is found in ch. 934, F.S. ("Security of Communications"). These provisions are guided, under the preemption doctrine, by federal provisions in Chapter 119 of Title 18, U. S. Code, Sections 2510 - 2522 ("Interception of Wire, Oral and Electronic Communications") and Chapter 121 of Title 18, U. S. Code, Sections

2701 – 2711 ("Stored Wire and Electronic Communications and Transactional Records Access").

Requirements for a court-authorized interception of communication include:

A showing that the applicant is authorized by law to seek the order. An intercept application must be in writing, upon oath/affirmation, to a judge of competent jurisdiction, stating the applicant's authority to apply. (s. 934.09(1), F.S.)

No interception order can be sought unless specifically authorized by one of the "authorizing officials" listed in the statute. (s. 934.09(1)(a), F.S.)

A showing that the officer is empowered to investigate one of the specifically listed offenses for which an intercept order is available [responsibility to investigate the particular offense (one included in a specifically enumerated list as being subject to interception)]. (s. 934.07, F.S.)

A full and complete statement of probable cause supporting the application. There must be a careful statement of facts and circumstances relied on by the applicant, which meet the "probable cause" proof standard as to the following:

Details as to the particular offense(s) involved.
Particular description of the nature/location of facilities from which, or where communications are to be intercepted (unless excepted).
Type of communications to be intercepted.
Identity of the person(s), if known, committing the offense and subject to being intercepted. (s. 934.09(1)(b), F.S.)

A showing that other investigative techniques have been exhausted (a unique requirement for communications interceptions). The application must demonstrate an "exhaustion of investigative techniques" as to all other investigative efforts and procedures tried and failed, and/or why other procedures reasonably appear unlikely to succeed if tried or are too dangerous. (s. 934.09(1)(c), F.S.)

An indication of how long the intercept is anticipated to last. If the interception should not automatically terminate upon first obtaining the described type of communication, then the application must provide a particular description of facts establishing probable cause that more communications of the same type will continue. (s. 934.09(1)(d), F.S.)

An indication whether there has been a prior interception. The application must state known facts regarding all known prior applications for interception regarding same persons, facilities, or places and the action taken by the judge on each such prior application. (s. 934.09(1)(e), F.S.)

The reviewing judge may "require more information." The judge may require applicant to furnish additional testimony or documentary evidence is support of the application. (s. 934.09(2), F.S.)

Once an intercept is authorized, all involved have a duty to "minimize" the interception by doing "spot listening" to determine whether the nature of the communication has turned to that sought as evidence. If the communication is not of evidentiary value, "listening" is not continuous, but remains in a "sampling" mode until the conversation becomes of evidentiary value (if at all). Otherwise privileged communications do not lose their privileged character, unless made in furtherance of crime. (s. 934.08(4), F.S.)

The judge's order must specify:

The identity of person(s), if known, whose communications are to be intercepted.
The nature and location of facilities/place for interception (unless excepted).
The type of communications and offense(s) for which interception is allowed.
The identity of the agency or agencies authorized to intercept communications.
The identity of official who authorized the application.
The period of time for interception and the termination parameters. (s. 934.09(4), F.S.)

Once approved, the interception must be prompt and limited to the mission defined in the order. There is a 30-day limit unless extended by the court. The issuing court's order is to be executed as soon as practicable. The interception shall not be longer than necessary to achieve objectives and in any event no longer than 30 days, unless by court-ordered extension. The interception must be conducted in such a way as to "minimize" interception of communications not authorized by order. (s. 934.09(5), F.S.)

The Court issuing the intercept order may continue ongoing monitoring of the progress of the investigation. The court may require that periodic reports be made to the court to show what progress has been made and the need for continued interception. (s. 934.09(6), F.S.)

Contents of communications intercepted must be recorded and protected from alteration or editing. The recordings are to be available to the issuing judge upon expiration of the interception order or end of the prosecution of a case based on the evidence for sealing the recordings. Sealed recordings are preserved a minimum of ten years as required by law. Duplicates may be used as allowed by the court. (s. 934.09(8), F.S.)

No later than 90 days after interception is complete (unless the time is extended by the court), a statutory notice is to be provided to parties whose communications were intercepted. (s. 934.09(8), F.S.) The notification, coupled with the required preservation of the interception recordings, assures that parties whose communications were intercepted can review the actions of those involved to determine compliance with the law. There are remedies for parties aggrieved by interception (s. 934.09(10), F.S.); civil remedies for violations (s. 934.10, F.S.); and criminal penalties for violations (s. 934.03, F.S.).

Both federal and Florida law allow for an "emergency intercept," under limited circumstances, but the emergency actions must be followed up with the written application and order within 48 hours. (s. 934.09(7), F.S.)

D. AMENDMENTS TO CHAPTER 934, F.S., IN 2001 SPECIAL SESSION C

In 2001 Special Session C, the Legislature amended ch. 934, F.S., as follows:

Amended s. 934.07, F.S., to provide that the Governor, the Attorney General, the Statewide Prosecutor, or any State Attorney may authorize an application to a judge of competent jurisdiction for the interception of wire, oral, or electronic communication by:

The Department of Law Enforcement or any law enforcement agency 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 aircraft piracy or solicitation to commit any violation of the laws of this state relating to crimes specifically enumerated in the statute as crimes for which an intercept may be ordered.

The Department of Law Enforcement 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 a conspiracy or solicitation to commit such act.

Amended s. 934.09, F.S., to provide an additional exemption from the requirement that an application for an interception identify the facilities from which, or the place where, the communication is to be intercepted. This exemption relates to a person whose communications are to be intercepted when the person has removed, or is likely to remove, himself or herself to another judicial circuit within the state.

Amended s. 934.09, F.S., to provide that the courts may authorize continued interception within this state in investigations of acts of terrorism. The continued interception can occur both within and outside the jurisdiction of the court authorizing the interception, if the original interception occurred within that court's jurisdiction.

The provisions of the bill (SB 12-C) took effect upon becoming law but are only effective until July 1, 2004. *See* ch. 2001-359, L.O.F.

E. CASE LAW RELEVANT TO CONTINUED INTERCEPTION

In *State v. McCormick*, 719 So.2d 1220 (Fla. 5th DCA 1998), the appellate court addressed an issue relating to the jurisdiction or authority of a Melbourne police detective to conduct an interception. The Melbourne Police Department wanted to establish a listening post in its jurisdiction (Melbourne), although the target cell phone was primarily in another jurisdiction (the subscriber was in Merritt Island). The State lost on this issue at the circuit court level. The appellate court determined that an "interception" of a cell phone takes place at either the location of the telephone or the site where law enforcement listens to and records the call. Therefore, the

Melbourne Police department had jurisdiction based on their having the listening post in Melbourne.

It is unclear whether the issue of a court's authority to order continued interception outside the court's territorial jurisdiction was actually or directly addressed in *McCormick*. Both Melbourne and Merritt Island were within the territorial jurisdiction of the court ordering the intercept. However, a number of cases cited as authority by the court appear to indicate that courts do have this authority.

There appears to be instances in which the application or authority of a circuit court's order extends beyond the court's territorial jurisdiction: arrest warrants; ne exeat orders; special maritime jurisdiction over crimes occurring outside Florida's territorial waters; and certain child welfare orders (e.g., where a circuit court acquires jurisdiction of a minor as an ancillary phase of a divorce proceeding and enters an order determining custody of the minor, and then subsequently amends its order changing custody of the minor, even though the minor is not within the court's territorial jurisdiction). These instances, by analogy, and policy and utility arguments may support the extraterritorial jurisdiction issue.

A different view might be that an intercept order is more analogous to, or actually constitutes, a search and seizure. There appears to be little (if any) support for seeking a search warrant from a judge in one circuit for property in another circuit. There appears to be no authority for a circuit court to issue a search warrant for a location outside the territorial jurisdiction of that court.

A counterargument to this view is that communications and property are apples and oranges. In *U.S. v. Burford*, 755 F. Supp. 607 (S.D.N.Y), the defendant, relying on *Weinberg v. United States*, 126 F.2d 1004 (2nd Cir. 1942), argued that "under Art. III, Section 2 and the Sixth Amendment of the United States Constitution, a district court is without power to issue search warrants or wiretap orders that reach beyond the territorial limits of its district." The court rejected this argument, stating:

> While *Weinberg* does stand for the proposition that as a general rule search warrants must be used in the jurisdiction where they are issued, we find this argument unpersuasive as applied to electronic surveillance. Search warrants are issued to permit seizure of tangible physical evidence, which is, by definition, in only one location. Wiretaps, in contrast, involve seizure of transitory intangible evidence. This is not a situation where Judge Carter authorized a seizure of the telephone in Maryland, as would be the analogous situation to the fact pattern in the *Weinberg* case. Rather, these were conversations that began in Maryland and were aurally acquired, or seized, in New York.

Additionally, the federal district court in *Burford* believed that the policies underlying electronic surveillance under Title III were "to alleviate the divergent practices among different jurisdictions in seeking and executing wiretap orders" and to "protect individual privacy rights." "While the Congress recognized the need for the government to use electronic surveillance devices, it was also concerned about abuses to an individual's right to privacy in the home. *See Giordano*, 416 U.S. at 520, 94 S.Ct. at 1829. Protecting unwarranted intrusion into an

individual's privacy is enhanced when orders are issued and wires are intercepted in one jurisdiction."

Similarly, the federal appellate court in *U.S. v. Rodriguez*, 112 F.3d 849 (2nd Cir. 1992) stated:

> Where the authorities seek to tap telephones in more than one jurisdiction and to monitor them in a single jurisdiction, there are sound policy reasons for permitting a court in the jurisdiction where all of the captured conversations are to be heard to grant the authorization. One of the key goals of Title III is the protection of individual privacy interests from abuse by law enforcement authorities. *See* generally, S.Rep. No. 1097, 90th Cong.2d Sess., reprinted in 1968 U.S.Code Cong. & Admin.News 2112, 2185; *United States v. Giordano*, 416 U.S. 505, 514-23, 94 S.Ct. 1820, 1826-30, 40 L.Ed.2d 341 (1974). For example, Title III requires that a wiretap authorization not allow the period of interception to be "longer than is necessary to achieve the objective of the authorization." 18 U.S.C. [s.] 2518(5). If all of the authorizations are sought from the same court, there is a better chance that unnecessary or unnecessarily long interceptions will be avoided. We doubt that Congress intended to eliminate this possibility.

Courts are not of one accord on this extraterritorial jurisdiction issue. There are some cases which arguably may be read to suggest that "seizure" or "acquisition" (of aural communication) does occur, and that the interception is at the place where the communication is initially obtained, regardless of where the communication is ultimately heard. *See e.g., U.S. v. Nelson*, 837 F.2d 1519 (11th Cir. 1988); *State v. Mozo*, 655 So.2d 1115 (Fla. 1995); *Koch v. Kimball*, 710 So.2d 5 (Fla. 2nd DCA 1998); and *Castillo v. Texas*, 810 S.W. 2d 180 (Tex. Crim. App. 1990).

Further, some courts have taken the approach that the interception may potentially occur at multiple locations or jurisdictions (location of phone or location of monitoring, if different); therefore, judges from several jurisdictions might be able to authorize an order for interception even for phones not physically in their jurisdiction, as long as a listening post is in their jurisdiction *See e.g., United States v. Ramirez*, 112 F.3d 849, 852 (7th Cir.1997) (upholding the authority of a federal district court in Wisconsin to issue an intercept order on a cellular phone where the phone and listening post were in Minnesota. The court discussed the mobility of the cellular phone and noted that "interception takes place both where the phone is located (including, we suppose, although we can find no cases, where the receiving phone is located) and where the scanner used to make the interception is located.")

III. Effect of Proposed Changes:

Section 1.
This section amends s. 934.02(1), F.S. ("Definitions") to:

> Amend the definition of "wire communication" to delete reference to electronic storage of such communication. (This change mirrors 18 U.S.C. 2510(1), as amended by Section 209 of the USA Patriot Act.)

Create the definition of "judge of a competent jurisdiction." (Section 220 provides that the term "court of a competent jurisdiction" has the same meaning assigned by 18 U.S.C. 3127, and includes any federal court within that definition, without geographic limitation. The definition in the CS is similar to the federal definition, but references the applicable state courts.)

Amend the definition of "pen register" to specify it is 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. It is further specified that 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. (This change mirrors 18 U.S.C. 3127(3), as amended by Section 216 of the USA Patriot Act.)

Amend the definition of "trap and trace device" to specify that it is 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. (This change mirrors 18 U.S.C. 3127(4), as amended by Section 216 of the USA Patriot Act.)

Define "foreign intelligence information" to mean information, whether or not concerning a United States person, as that term is defined in 50 U.S.C. 1801, which relates to: 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; sabotage or international terrorism by a foreign power or an agent of a foreign power; clandestine intelligence activities by an intelligence service, a network of a foreign power, or an agent of a foreign power; or 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. (This change mirrors the definition of the same term in 18 U.S.C. 2510(19), as created by Section 203 of the USA Patriot Act.)

Define "protected computer" to mean a computer: for the exclusive use of a financial institution or governmental entity; 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 used in interstate or foreign commerce or communication, including a computer located outside the United States. (Section 217 creates 18 U.S.C. 2510(20), which provides that the term "protected computer" has the same meaning as set forth in 18 U.S.C. 1030. The definition in the CS mirrors 18 U.S.C. 1030, as amended by section 814 of the USA Patriot Act.)

Define "computer trespasser" to mean 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. (This change mirrors the definition of the same term in 18 U.S.C. 2510(21), as created by Section 217 of the USA Patriot Act.)

Section 2.
This section amends s. 934.03, F.S. ("Interception and disclosure of wire, oral, or electronic communications prohibited") to provide that it is not unlawful under ss. 934.03-934.09, F.S., 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: the owner or operator of the protected computer authorizes the interception of the communications of the computer trespasser; the person acting under color of law is lawfully engaged in an investigation; 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 the interception does not acquire communications other than those transmitted to, through, or from the computer trespasser. (This change mirrors language created in 18 U.S.C. 2511(2) by Section 217 of the USA Patriot Act.)

Section 3.
This section amends s. 934.07, F.S. ("Authorization for interception of wire, oral, or electronic communications"), as amended by section 1, ch. 2001-359, L.O.F., to provide that 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, F.S., an order authorizing or approving the interception of, wire, oral, or electronic communications by FDLE or any law enforcement agency 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 a felony violation of ss. 790.161-790.166, F.S. These sections pertain to offenses involving bombs, destructive devices, and weapons of mass destruction.

(Current Language in 18 U.S.C. 2516(1) provides authority to intercept communications regarding illegal explosives. Section 201 of the USA Patriot Act creates language in 18 U.S.C. 2516(1) that provides authority to intercept communications regarding weapons of mass destruction. There is no direct Florida counterpart to these federal provisions, but the reference to "any felony violation of ss. 790.161-790.166 inclusive" captures the federal intent.)

This section also allows FDLE, consistent with current law, to utilize resources to effectively investigate acts of terrorism, including the use of personnel from other agencies who would be acting at the direction of FDLE. (Similar language appears in s. 934.09, F.S) FDLE states that an example of "'other assisting personnel' might be a linguist who is familiar with a particular dialect being spoken by those whose communications are being intercepted."

This section also provides that if, during the course of an interception of communications by a law enforcement agency as authorized under paragraph (1)(a) of s. 934.07, F.S., 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 must promptly notify FDLE and apprise it of the contents of the intercepted communications. The agency notifying FDLE may continue its previously authorized interception with appropriate minimization, as applicable, and may otherwise assist FDLE, as provided in paragraph (1)(b) (authorizing an application for an interception by FDLE in an investigation of an act of terrorism or in furtherance of such act or a conspiracy or solicitation to commit such act).

Upon its receipt of information of the contents of an intercepted communications from a law enforcement agency, FDLE must promptly review the information to determine whether the information relates to an actual or anticipated act of terrorism. 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), FDLE may make application for the interception of wire, oral, or electronic communications consistent with paragraph (1)(b). FDLE may make an independent new application for interception based on the contents of the intercepted communications. Alternatively, FDLE 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 FDLE. In carrying out its duties under this section, FDLE may use the provisions for an emergency interception provided in s. 934.09(7), F.S., if applicable under statutory criteria.

(As indicated by the amendments in 2001 Special Session C, the Legislature intended FDLE to play a primary role in any state or local terrorism investigation. The added paragraphs (2)(a) and (2)(b) specify the respective obligations of FDLE and another law enforcement agency when that other agency's interception develops a "terrorism" aspect. The amendment helps facilitate coordination between FDLE and the other agency and ensure FDLE's continuing and meaningful involvement in terrorism investigations.)

Section 4.
This section amends s. 934.09, F.S. ("Procedures for interception of interception of wire, oral, or electronic communications"), as amended by section 2, ch. 2001-359, L.O.F. The amendment authorizes application for an intercept if the applicant reasonably believes an emergency exists that involves conspiratorial activities threatening the security interest of the nation or state. (This provision is similar to a provision in 18 U.S.C. 2518(7), but also adds conspiratorial activities that threaten the security interest of the state.)

This section also modifies and extends a provision passed in 2001 Special Session C that provides that a court may authorize continued interception within this state, both within and outside its jurisdiction, if the original interception occurred within its jurisdiction and only involves investigations of acts of terrorism. The amendment substitutes the term "judge of competent jurisdiction" for the current and initial reference to "the court" (see Section 1 for an explanation of this term) and provides that this judge may authorize interception within this state,

whether the interception is within or outside the court's jurisdiction, if the application for an 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 and the communications 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 sought.

(This language does not directly track the USA Patriot Act, which allows the intercept order to have extended authority when the criminal activity extends beyond the court's normal geographic limit, provided that some of the activity does in fact occur within the issuing court's jurisdiction. The CS contains a similar requirement but adds an additional requirement that the application for an interception show that the communication is occurring or will likely occur within the jurisdiction of the court issuing the intercept order. According to the General Counsel of FDLE, this language is problematic: *". . . [W]e cannot always be assured that a communication will occur in whole or in part in a jurisdiction. This is due to computer switching and high technology now in place. We can intercept communications via a court order, but we are not always sure where the person talking is going to be when he talks. Example: Major drug conspiracy organization working out of Tampa, using couriers with cell phones who begin their conversations when they arrive at their points of distribution elsewhere in the state. The majority of investigative efforts will be in Hillsborough County, and that's the most likely court to approach for intercept order, since the organization is based there. However, there's no guarantee that the cell phones will result in a communication "in whole or in part" in Hillsborough County, although the communications will be by associates of the drug organization based in Hillsborough. [The amendment] . . . could result in what otherwise would be an appropriate court being excluded, or worse still, communications being suppressed because we were wrong when we thought communications would occur "in whole or in part" in the court's jurisdiction when, by reason of technology, they occurred elsewhere*.) (bracketed information provided by analyst)

Section 5
In 2001 Special Session C, the Legislature specified that the "continued interception" provision it was passing (see previous section) would sunset July 1, 2004. This section provides that effective July 1, 2004, paragraph (b) of subsection (11) of s. 934.09, F.S., as amended by this act and by section 3, ch. 2001-359, L.O.F., is amended. The amendment includes the amendments to paragraph (b) of subsection (11) that are contained in Section 4. The practical effect is that the language previously indicated for sunsetting will not sunset in 2004, and will be retained or amended by this act.

Section 6.
This section amends s. 934.08, F.S. ("Authorization for disclosure and use of intercepted wire, oral, or electronic communications"). The amendment tracks language in Section 203 of the USA Patriot Act that provides authority to share criminal investigative information; specifically, it authorizes an investigative or law enforcement officer or attorney for the Government who, by authorized means, obtains knowledge of the contents of any wire, oral, or electronic communication derived from the contents of any wire, oral, or electronic communication to disclose the contents or evidence to a federal law enforcement, intelligence, national security, national defense, protective or immigration official to assist the official receiving that information in the performance of his or her official duties. (The changes are comparable to the

changes made in Section 203 of the USA Patriot Act but also include the state counterparts to the specified federal officials, and do not include an attorney for the Government as a person authorized to disclose the contents of the communication.)

Section 7
This section amends s. 934.22, F.S. ("Disclosure of contents") to modify provisions dealing with release of the contents of communications in the custody of a provider of a remote computing service or electronic communications service to the government and others. It provides for special emergency release to the government or others of a record or other information pertaining to a subscriber/customer of identified providers in an emergency involving immediate danger of death or serious physical injury. (The changes are comparable to language created in 18 U.S.C. 2702 by Section 212 of the USA Patriot Act.)

Section 8
This section amends s. 934.23, F.S. ("Requirements for governmental access") to add the term "wire" to several subsections to broaden the types of communications providers that are covered by those subsections.

This section also makes several modifications to s. 934.23, F.S., to set forth the type of legal process needed in order for an investigative or law enforcement officer to obtain certain records from a provider of electronic communication service or remote computing service. It sets forth a new and expanded listing of the types of records contemplated to be released upon receipt of the appropriate legal documents. (The changes are comparable to language created in 18 U.S.C. 2703 by Sections 209, 210, and 212 of the USA Patriot Act.)

Section 9.
This section amends s. 934.27, F.S. ("Civil action; relief; damages; defenses) to provide that a good faith reliance on 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), F.S., is a complete defense to any civil or criminal action brought under ss. 934.21-934.28, F.S. The CS extends relief from civil liability to cases in which an officer requests that records be preserved in accordance with current law. This provision extends protections to the providers of services that can include individual citizens or companies. (This change is comparable to the language created in 18 U.S.C. 2707(e)(1) by Section 815 of the USA Patriot Act.)

Section 10.
This section amends s. 934.31, F.S. ("General prohibition on pen register and trap and trace device use; exception") to add the phrase "trap and trace" to this section along with other limitation provisions to make it clear that an investigative or law enforcement officer shall use technology reasonably available to him or her which restricts the recording or decoding of electronic or other impulses to the dialing (now also adds routing, addressing) and signaling information used in the processing and transmitting of wire or electronic communication so as not to include the contents of any wire or electronic communications.

(The changes are comparable to language created in 18 U.S.C. 3121(c) by Section 216 of the USA Patriot Act.)

Section 11.
This section amends s. 943.33, F.S. ("Issuance of an order for a pen register or a trap and trace device") to require an officer serving an order for a pen register or a trap and trace device, if requested, to provide the person or entity served with written or electronic certification that the order applies to that person or entity if they are not specifically named in the order. According to FDLE, this provision is important to service providers, whether telecommunications businesses or internal service providers, as it gives them the right to demand certification that the order applies to them, thus triggering their ability to claim protection from civil liability due to their good-faith execution of a lawful order.

This section also adds the phrase "or other facility" and the devices being "applied" to note that this section can relate to more than just telephones and may entail the application of the devices to the telephone line or other facility rather than the attachment of the devices to the telephone lines or other facility. Section 943.33, F.S., generally requires such companies to provide assistance to the officer making the application and requires them not to disclose the existence of the device or investigation.

This section also sets forth detailed provisions dealing with requirements needed when an investigative or law enforcement officer implements an ex parte order by installing and using his own pen register or trap and trace device on a packet-switched data network of an electronic communications service to the public. The agency must insure that a record will be kept to identify the officers that installed the device, and the date and time of same, and who accessed same, date and time of uninstallation, configuration, modifications, duration device is used and information collected. If device is automated, the records shall be maintained electronically. Records maintained pursuant to s. 943.33, F.S., shall be provided ex parte and under seal to the court that entered the order within 30 days after termination, excluding any extensions thereof.

(The changes are comparable to language created and amended in 18 U.S.C. 3123 by Section 216 of the USA Patriot Act.)

Section 12.
This section amends s. 934.34, F.S. ("Assistance in installation and use of a pen register or trap and trace device") to add the phrase "or other facility" to note that this section can relate to more than just telephones. (This change is comparable language created in 18 U.S.C. 3124(b) by Section 216 of the USA Patriot Act.)

Section 13.
This section provides that this act shall take effect upon becoming a law.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Economic Impact and Fiscal Note:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

None.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Amendments:

None.