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: SB 12-C

SPONSOR: Senators Brown-Waite and Smith

SUBJECT: Interception of Communications

DATE: November 27, 2001 REVISED: _____ _____ _____ _____

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

I. Summary:

Senate Bill 12-C amends 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:

1. 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.

2. The Department of Law Enforcement for the investigation of the offense as to which application is made when such interception may provide or has provided evidence of the commission of any offense that may be an act of terrorism or in furtherance of an act of terrorism or evidence of any conspiracy or solicitation to commit any such violation. The bill defines the term “terrorism” for purposes of this section.

The bill also amends s. 934.09, F.S., to provide an additional exemption from the requirement that an application for an intercept 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.

The bill further amends 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 take effect upon becoming law but are only effective until July 1, 2004.

This bill amends ss. 934.07 and 934.09, F.S.

II. Present Situation:

A. Section 934.07

Section 934.07, F.S., provides that the Governor, the Attorney General, the Statewide Prosecutor, or any State Attorney may authorize an application to a judge of competent jurisdiction for an order authorizing the interception of wire, oral, or electronic communications by the Department of Law Enforcement or any law enforcement agency (as defined in s. 934.02, F.S.) 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 following offenses: murder, kidnapping, arson, gambling, robbery, burglary, theft, dealing in stolen property, criminal usury, bribery, or extortion; any violation of chapter 893, F.S.; any violation of the provisions of the Florida Anti-Fencing Act; any violation of chapter 895, F.S.; any violation of chapter 896, F.S.; any violation of chapter 815, F.S.; any violation of chapter 847, F.S.; any violation of s. 827.071, F.S.; any violation of s. 944.40, F.S.; or any conspiracy to commit any violation of the laws of this state relating to such offenses.

B. Section 934.09

Section 934.09(1), F.S., provides that each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under ss. 934.03-934.09, F.S., shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Among the information the statute specifies must be included is a particular description of the nature and location of the facilities from which, or the place where, the communications are to be intercepted. s. 934.09(1)(b), F.S. Subsection (11) contains exemptions to this requirement. *Id*.

Section 934.09(3), F.S., provides that upon application for an interception, the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting, and outside such jurisdiction but within the State of Florida in the case of a mobile interception device authorized by the judge within such jurisdiction, if the judge determines on the basis of the facts submitted by the applicant that:

(a) There is probable cause for belief that an individual is committing, has committed, or is about to commit an offense as provided in s. 934.07, F.S.
(b) There is probable cause for belief that particular communications concerning that offense will be obtained through such interception.
(c) Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.

(d) Except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

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

(a) In the case of an application with respect to the interception of an oral communication:
1. The application is by an agent or officer of a law enforcement agency and is approved by the Governor, the Attorney General, the statewide prosecutor, or a state attorney.
2. The application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted.
3. The judge finds that such specification is not practical.

(b) In the case of an application with respect to a wire or electronic communication:
1. The application is by an agent or officer of a law enforcement agency and is approved by the Governor, the Attorney General, the statewide prosecutor, or a state attorney.
2. The application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility.
3. The judge finds that such showing has been adequately made.
4. The order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

C. 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 that 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 appear 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 is 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.")

D. Definition of "Terrorism"

There is presently no state definition of the term "terrorism."

Recent federal legislation amends 18 U.S.C s. 2331 to create a definition of "domestic terrorism." *See e.g.*, Section 802, H.R. 2975, the "USA Act of 2001" (107th Congress). The definition of "domestic terrorism" in 18 U.S.C. s. 2331, as amended by the federal legislation is as follows:

(5) the term 'domestic terrorism' means activities that—

> (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
>
> (B) appear to be intended—
>
> > (i) to intimidate or coerce a civilian population;
> >
> > (ii) to influence the policy of a government by intimidation or coercion; or
> >
> > (iii) to affect the conduct of government by mass destruction, assassination, or kidnapping; and
>
> (C) occur primarily within the territorial jurisdiction of the United States.

The definition of "domestic terrorism" is similar, but not identical, to the definition of "act of terrorism" in Title 18 U.S.C. s. 3077:

(1) "act of terrorism" means an activity that—
(A) involves a violent act or an act dangerous to human life that is a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; and
(B) appears to be intended—
(i) to intimidate or coerce a civilian population;
(ii) to influence the policy of a government by intimidation or coercion; or
(iii) to affect the conduct of a government by assassination or kidnapping . . .

III. Effect of Proposed Changes:

Senate Bill 12-C amends 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:

1. 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 crimes enumerated consist of: murder, kidnapping, arson, gambling, robbery, burglary, theft, dealing in stolen property, criminal usury, bribery, or extortion; any violation of chapter 893, F.S.; any violation of the provisions of the Florida Anti-Fencing Act; any violation of chapter 895, F.S.; any violation of chapter 896, F.S.; any violation of chapter 815, F.S.; any violation of chapter 847, F.S.; or any violation of s. 827.071, F.S.

2. The Department of Law Enforcement for the investigation of the offense as to which application is made when such interception may provide or has provided evidence of the commission of any offense that may be an act of terrorism or in furtherance of an act of terrorism or evidence of any conspiracy or solicitation to commit any such violation.

The bill also defines the term "terrorism" for purposes of s. 775.31, F.S. The definition in the bill contains some of the same features of Title 18 U.S.C. s. 2331, as amended by Section 802, H.R. 2975, the "USA Act of 2001" (107th Congress) and Title 18 U.S.C. s. 3077, and some features that are unique to the definition in the bill.

The definition of "terrorism" in the bill is as follows:

775.30 Terrorism; definition.—As used in the Florida Criminal Code, the term "terrorism" means an activity that:

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

(b) Involves a violation of s. 815.06; and

(2) Is intended to:

(a) Intimidate, injure, or coerce a civilian population;

(b) Influence the policy of a government by intimidation or coercion; or

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

Some of the substantial differences between the definition in the bill and the federal definitions are described in the following remarks.

To constitute "terrorism," the violent act or act dangerous to human life which is a federal criminal violation or Florida crime, the act must also have been *intended* for one of three specified purposes. In the federal sections, it is only necessary that the specified act *appear to be intended* for the specified purposes.

In addition to a violent act (Section 3077) or an act dangerous to human life (Sections 2331 and 3077) which is a criminal violation, the definition in the bill includes a violation of s. 815.06, F.S. (computer crimes). Apparently, this inclusion is to address cyberterrorism.

The specified act is an act of "domestic terrorism" (Section 2331) or an "act of terrorism" (Section 3077) if it appears to be intended to intimidate or coerce a civilian population. In the bill, the specified act is an act of "terrorism" if it is intended to intimidate, *injure*, or coerce a civilian population.

The specified act is also an act of "domestic terrorism" (Section 2331) or an "act of terrorism" (Section 3077) if it appears to be intended to affect the conduct of government by mass destruction (Section 2331), assassination (Sections 2331 and 3077), or kidnapping (*id.*). The definition in the bill does not include "mass destruction"; it includes destruction to property. Further, in addition to including assassination and kidnapping, the bill includes murder and aircraft piracy. Assassination is not a specific crime in Florida (the act would constitute murder), but it is a specific federal crime, and the definition in the bill includes violent acts that are federal crimes. *See* Title 18 U.S.C. s. 351 (Congressional, Cabinet, and Supreme Court assassination, kidnapping, and assault) and 18 U.S.C. s. 1751 (Presidential and Presidential staff assassination, kidnapping, and assault).

Under Section 2311, the relevant act must also "occur primarily within the territorial jurisdiction of the United States." Section 3077 includes the specified act that "would be a criminal violation if committed within the jurisdiction of the United States or of any State. . . ." The definition in the bill does not include these provisions. It appears that the provision in Section 2311 is there to distinguish the definition of "domestic terrorism" in that section from the definition of "international terrorism" in that section. The provision in Section 3077 is relevant to that section, because Section 3077 appears in Chapter 204 of Part II of Title 18, which relates to rewards for information concerning terrorist acts and espionage. Neither provision is relevant to the state definition.

The bill also amends s. 934.09, F.S., to provide an additional exemption from the requirement that an application for an intercept 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.

The bill further amends 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 take effect upon becoming law but are only effective until July 1, 2004.

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.