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 180

SPONSOR: Criminal Justice Committee and Senator Silver

SUBJECT: Computer Crimes

DATE: April 3, 2001 REVISED: _____ _____ _____ _____

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

I. Summary:

The Committee Substitute for Senate Bill 180 creates the "Computer Crimes Control Act" to address the issue of problems and damages caused by persons who knowingly interfere with computer operations of other persons, organizations, business and financial entities and governmental agencies. This would:

- Express the Legislature's findings and intent with regard to computer crimes;
- Define several terms relevant to computer activity;
- Describe the crime of "computer interference" with penalties; and
- Establish rules for civil actions by victims of computer crimes.

This bill prohibits computer interference, and describes it as knowingly and without permission disrupting computer services, or introducing a computer contaminant (virus) into any computer, computer system, or computer network.

This act takes effect on October 1, 2002.

This bill creates an as yet unnumbered section of the Florida Statutes.

II. Present Situation:

Chapter 815, F.S., contains the "Florida Computer Crimes Act" which was enacted in 1987. ch. 78-92, L.O.F. This statute was drawn directly from the session law and has been amended in a few places over the past 20 years. There are several other sections of the Florida Statutes dealing with computers and related matters. Section 847.0135, F.S., the "Computer Pornography and

Child Exploitation Prevention Act of 1986" prohibits two offences; using a computer to lure children into sexual conduct and posting child pornography.

FLORIDA COMPUTER CRIMES ACT (Chapter 815, F.S.)

Legislative intent

In 1978, the Legislature found that computer-related crime was a growing problem in the business and government sectors; that the potential for losses could be far greater than in traditional white collar crimes, especially in the financial community; and that there is a need for specific law to address computer crimes. This was written before the advent of the personal computer, when virtually all computers were main frames used by government or large businesses. Today, almost half of all family homes contain at least one computer and their ability to access the Internet and one another grows rapidly.

Definitions

The statute defines several computer terms such as:

- "computer" means an internally programmed data processing device;
- "computer program" means instructions for the computer to process data;
- "computer system" means a set of related computers;
- "computer network" means a set of related and connected computers and other devices with the capability to transmit data; and
- "property" means data, computers programs, and such, but also includes financial instruments such as bank drafts, and marketable securities.

There is no definition or mention of the Internet, a personal computer, e-mail, or the World Wide Web in ch. 815, F.S.

Offenses

Chapter 815, F.S., creates offenses in three categories:

1. offenses against intellectual property, s. 815.04, F.S.;
2. offenses against computer equipment or supplies, s. 815.05, F.S.; and
3. offenses against computer users, s. 815.06, F.S.

All three of the offenses have similar language that prohibits a person from "willfully, knowingly, and without authorization" accessing a computer or computer system, stealing or damaging computer related property, financial instruments, or other computer data.

Section 815.04, F.S., prohibits offenses against "intellectual property" which s. 815.03(1), F.S., defines as data, including programs. The statutes prohibit damaging or altering data or programs. This is punished as a third degree felony, unless done to defraud or unlawfully obtain property, in which case it is punished as a second degree felony.

Section 815.05, F.S., prohibits offenses against computer equipment that causes damage to the actual computer. If the damage is less than $200, the offense is a misdemeanor. If the damage is between $200 and $1000, the offense is a third degree felony. If the damage is over $1000, the offense is a second degree felony.

Section 815.06, F.S., prohibits offenses against computer users, which causes the authorized user to be denied computer service. This is treated as a third degree felony, unless done to defraud or unlawfully obtain property, in which case it is punished as a second degree felony.

Section 815.07, F.S., provides that the laws in ch. 815, F.S., are not to be construed so as to prevent law enforcement from using other criminal laws to punish computer-related crimes where possible.

Computer Pornography and Child Exploitation Prevention Act of 1986

Section 847.0135, F.S., prohibits the use of a computer or the Internet to lure a child into sexual conduct. The statute goes on to prohibit collecting or sharing information about children with the intent to facilitate sexual conduct with a minor. The statute expresses that it is also illegal to possess, transmit, sell, or otherwise distribute a visual depiction of a child in sexual conduct. The offense is punished as a third degree felony. Section 847.0135(4), F.S., prohibits operating a computer on-line service and knowingly allowing others to violate this section. A violation of this section is punished as a misdemeanor, with a possible $2000 fine.

Other statutes that can be applied to computer crimes

According to the supervisor of the computer crimes division for the Department of Law Enforcement, several other statutes can be applied to many computer related crimes. Most of the crimes that are described in ch. 815, F.S., could be punished as some form of theft (ss. 812.014-812.081, F.S.), embezzlement (s.655.0322, F.S.), fraud (ch. 817, F.S.), or criminal mischief (s. 806.13, F.S.). The facts showing an offense was a computer-related crime do not require the state to prosecute the offense as a violation of ch. 815, F.S. s. 815.07, F.S.

Florida's capacity to investigate computer-related crime

The Department of Law Enforcement has an office dedicated to the investigation of computer crimes. The office includes a supervisor, 2 agents, 2 analysts, a systems administrator and a trainer/researcher. This office has jurisdiction over the entire state and assists local law enforcement as needed. According to the supervisor, a few of the larger counties and municipalities have some training and expertise in investigation of computer-related crimes. Most local law enforcement agencies will call on the Department of Law Enforcement to take the lead in these investigations. In some cases, the FBI or other federal agencies will conduct investigations, as many computer-related crimes are of an interstate nature.

III. Effect of Proposed Changes:

Committee Substitute for Senate Bill 180 would create a new and as of yet unnumbered section of the Florida Statutes to be called the, "Computer Crimes Control Act." This statute would

prohibit the offense of "computer interference," and describe it as knowingly and without permission disrupting computer services, or introducing a computer contaminant (virus) into any computer, computer system, or computer network. In addition to describing the offense of computer interference, this bill expresses the Legislature's findings with regard to computer crimes, defines several terms and establishes rules for civil actions by victims of computer interference.

Subsection 1 of the bill states that this law may be referred to as the "Computer Crimes Control Act."

Subsection 2 of this bill expresses the findings and intent of the Legislature as follows:

- The Legislature intends to expand legal protection for individuals, businesses, and governmental agencies from interference and damage to their computer systems.
- The Legislature finds that the growth in computer technology has been mirrored by a growth in computer crime and unauthorized access to computer systems.
- The Legislature finds that it is necessary to create law to protect the integrity of computer systems, the privacy of individuals, and the security of financial institutions and business concerns.

Subsection 3 of this bill defines several terms related to computers, some of which are:

- "access" to gain entry to or communicate with a computer system;
- "computer contaminant" means computer instructions (computer virus) designed to modify, damage, destroy, record, or transmit information within a computer system without the intent, permission, or knowledge of the owner; and
- "victim expenditure" means the costs the owner of the computer system incurred to verify that their computer system was altered or damaged by unlawful access.

Subsection 4 of this bill would create the offense of "computer interference." The bill describes computer interference, and describes it as knowingly and without permission disrupting computer services, or introducing a computer contaminant (virus) into any computer, computer system, or computer network. The bill prohibits:

- prohibits disrupting the computer services of the authorized users; and
- prohibits introducing a computer virus into a computer system.

Subsection 5 of this bill sets forth the penalties for violations of the prohibitions in subsection 4. Any person who violates subsection 4 would commit a second degree felony if the violation results in a "victim expenditure" of less than or equal to $5000 to verify computer damages, or a first degree felony if the violation results in a "victim expenditure" of more than $5000 to verify computer damages.

Subsection 6 of this bill would establish rules relating to civil actions by the victims of computer crimes, allow for attorney fees, and require student sanctions. In addition to any other civil remedy already available to the victims of crimes, this bill would allow the victims of computer

crimes to recover the "victim expenditure" defined in subsection 3 as the cost of verifying computer crime damages. Furthermore, the victim would be entitled to reasonable attorney fees. Paragraph (c) would require each community college, state university and academic institution to include in its student conduct rules a prohibition on computer crimes.

Subsection 7 of this bill would allow law enforcement agencies, pursuant to ss. 932.701-932.704, F.S., to acquire through legal forfeiture any computer property owned by the defendant and used in the commission of the computer-related crime.

Subsection 8 of this bill would provide that this law not be applicable to those persons who access their employers computer systems in the scope of their lawful employment.

Subsection 9 of this bill recognizes that the crime of computer interference can occur in more than one jurisdiction in the same incident. This section would allow the crime to be prosecuted in more than one jurisdiction.

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:

The Criminal Justice Estimating Conference has been asked to review this proposed legislation, but has not yet done so. It is possible that all of the crimes described in this bill could be prosecuted and punished under existing criminal statutes.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Amendments:

None.