

The Florida Senate
BILL ANALYSIS AND FISCAL IMPACT STATEMENT

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

Prepared By: The Professional Staff of the Committee on Communications, Energy, and Public Utilities

BILL: CS/SB 364

INTRODUCER: Communications, Energy, and Public Utilities and Senator Brandes

SUBJECT: Computer Crimes

DATE: February 04, 2014 REVISED: _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Telotte/Wiehle	Caldwell	CU	FAV/CS
2.	_____	_____	CJ	_____
3.	_____	_____	ACJ	_____
4.	_____	_____	AP	_____

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 364 recognizes that advancements in technology have led to an increase in computer related crimes while greatly extending their reach. The bill addresses this increase by updating terminology used to define these crimes and creating additional offenses.

Three crimes are added to “offenses against users of computer networks and electronic devices” including:

- Audio and video surveillance of an individual without that individual’s knowledge by accessing any inherent feature or component of a computer, computer system, computer network, or electronic device;
- Intentionally interrupting the transmittal of data to or from, or gaining unauthorized access to a computer, computer system, computer network, or electronic device belonging to a mode of public or private transit; and
- Disrupting a computer, computer system, computer network, or electronic device that affects medical equipment used in the direct administration of medical care or treatment to a person.

“Offenses against a public utility” are created in the bill and create two additional crimes, including:

- Gaining access to a computer, computer system, computer network, or electronic device owned, operated, or used by a public utility while knowing that such access is unauthorized; and
- Physically tampering with, inserting software into, or otherwise transmitting commands or electronic communications to a computer, computer system, computer network, or electronic device which cause a disruption in any service delivered by a public utility.

II. Present Situation:

Offenses against intellectual property

A person commits an offense against intellectual property, punishable as a third degree felony, if he does one of the following:

- willfully, knowingly and without authorization modifies or destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network; or
- willfully, knowingly and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in s. 812.081, F.S., or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network.

If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, the offense is elevated to a second degree felony.

Offenses against computer users

It is an offense against computer users, punishable as a third degree felony, to willfully, knowingly, and without authorization:

- Access or cause to be accessed any computer, computer system, or computer network; or
- Disrupt or deny or cause denial of computer system services to an authorized user of such computer system services, which in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another; or
- Destroy, take, injure, or damage equipment or supplies used or intended to be used in a computer, computer system, or computer network; or
- Destroy, injure, or damage any computer, computer system, or computer network; or
- Introduce any computer contaminant into any computer, computer system, or computer network.

It is a second degree felony to commit an offense against computer users and additionally do any of the following:

- Damage a computer, computer equipment, a computer system, or a computer network and the monetary damage or loss incurred as a result of the violation is \$5,000 or greater;
- Commit an offense for the purpose of devising or executing any scheme or artifice to defraud or obtain property; or
- Interrupt or impair a governmental operation or public communication, transportation, or supply of water, gas, or other public service.

Committing an offense against computer users in any manner which endangers a human life is punishable as a first degree felony.

III. Effect of Proposed Changes:

Section 1 amends s. 815.02, F.S., to add a statement of legislative intent to recognize “The proliferation of new technology has led to the integration of computer systems in most sectors of the marketplace through the creation of computer networks, greatly extending the reach of computer crime.”

Section 2 expands s. 815.03, F.S., to define the term “electronic devices” and include the devices in the definition of a “computer network”, which is a system that provides a medium for communication between one or more computer systems or electronic devices, including communication with an input or output device such as a display terminal, printer, or other electronic equipment that is connected to the computer system or electronic devices by physical or wireless telecommunication facilities. An “electronic device” is defined as a device that is capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data. These changes allow for devices other than the standard computer to be considered capable of being used to commit an offense. The bill also acknowledges the ability to form a computer network using wireless telecommunication facilities.

Section 3 amends s. 815.04, F.S., to include the term “electronic devices” in the existing definition of offenses against intellectual property.

SB 366, a linked bill, amends the existing public records exemption regarding trade secrets in s. 815.04, F.S., and takes effect the same day as SB 364 if adopted the same session.

Section 4 amends s. 815.06, F.S., and renames these offenses “offenses against users of computer networks and electronic devices.”

The definition of the term “person” is expanded for use in this section, to include:

- An individual;
- A partnership, corporation, association, or other entity doing business in this state, or an officer, agent, or employee of such entity; or
- An officer, employee, or agent of the state or a county, municipality, special district, or other political subdivision whether executive, judicial, or legislative, including, but not limited to, a department, division, bureau, commission, authority, district, or agency thereof.

The bill changes the criteria used to determine whether a person commits such a crime.

Current law provides that a person commits an offense against users of computer networks or electronic devices, which is punishable as a third degree felony, if he willfully, knowingly, and without authorization:

- Accesses or causes to be accessed by any computer, computer system, computer network, or electronic device with knowledge that such access of unauthorized; or

- Disrupts or denies or causes the denial or the ability to transmit data to or from an authorized user of such computer system or computer network services, which, in whole or in part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another.

The bill adds audio and video surveillance to this list, stating that “It is an offense to engage in audio or video surveillance of an individual without the individual’s knowledge by accessing any inherent feature or component of a computer, computer system, computer network, or electronic device, including accessing the data or information of a computer, computer system, computer network, or electronic device that is stored by a third party.”

If a person commits an offenses against users of a computer network and electronic devices and does either of the following, it is punishable as a first degree felony:

- Endangers a human life; or
- Disrupts a computer, computer system, computer network, or electronic device that affects medical equipment used in the direct administration of medical care or treatment to a person.

The bill provides that the section does not apply to a person who has acted pursuant to a search warrant authorized by law or when acting within the scope of his or her employment.

It is a third degree felony to commit an offense against users of computer networks and electronic devices. The punishment for the offense is elevated, and is punishable as a second degree felony, if a person commits an offense against users of computer networks and electronic devices, in addition to either of the following:

- Damages a computer, computer equipment or supplies, a computer system, or a computer network and the damage or loss is at least \$5,000; or
- Intentionally interrupts the transmittal of data to or from, or gains unauthorized access to, a computer, computer system, computer network, or electronic device belonging to any mode of public or private transit, as defined in s. 341.031, F.S.

Section 5 creates s. 815.061, F.S., to define offenses against public utilities. The term “public utility” in this section means each public utility and electric utility as those terms are defined in s. 366.02, F.S.; each water and wastewater utility as defined in s. 367.021, F.S.; each natural gas transmission company as defined in s. 368.103, F.S.; each person, corporation, partnership, association, public agency, municipality, cooperative, gas district, or other legal entity and their lessees, trustees, or receivers, now or hereafter owning, operating, managing, or controlling gas transmission or distribution facilities or any other facility supplying or storing natural or manufactured gas or liquefied gas with air admixture or any similar gaseous substances by pipeline to or for the public within this state; and any separate legal entity created under s. 163.01, F.S., and composed of any of the entities described in this subsection for the purpose of providing utility services in this state, including wholesale power and electric transmission services.

A person may not willfully, knowingly, and without authorization:

- Gain access to a computer network or other defined device owned, operated, or used by a public utility while knowing that such access is unauthorized, which is punishable as a third degree felony; or
- Physically tamper with, insert software into, or otherwise transmit commands or electronic communications to a computer, computer system, computer network, or electronic device which causes a disruption in any service delivered by a public utility, which is punishable as a second degree felony.

Similar infractions are addressed in s. 815.06, F.S., which states that it is an offense against computer users if a person interrupts or impairs a governmental operation or public communication, transportation, or supply of water, gas, or other public service. However, s. 815.06, F.S., does not expressly include public utilities.

Technical and conforming changes are made throughout the bill.

Section 6 states that the bill takes effect October 1, 2014.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

The bill may provide better protection against economic loss to owners and users of computers, computer systems, and electronic devices.

C. Government Sector Impact:

The bill may result in additional arrests, prosecutions, and incarcerations. The economic impact of these potential increases is uncertain.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 815.02, 815.03, 815.04, and 815.06.

This bill creates section 815.061 of the Florida Statutes.

IX. Additional Information:

- A. **Committee Substitute – Statement of Substantial Changes:**
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS by Communications, Energy, and Public Utilities on February 04, 2014:

The CS/SB 364 provides that the term “public utility” is not limited to the definition found in s. 366.02, F.S., but also includes additional types of utilities such as water and wastewater utilities, natural gas pipelines, natural gas storage, and supply facilities, or utilities under the direction of a governmental owned authority (Facilities that serve a public purpose and are necessary for the security and wellbeing of the public.)

- B. **Amendments:**

None.