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 Appropriations

BILL:	CS/CS/CS/SB 364
INTRODUCER:	Appropriations Committee (Recommended by Appropriations Subcommittee on Criminal and Civil Justice); Criminal Justice Committee; Communications, Energy, and Public Utilities Committee; and Senator Brandes
SUBJECT:	Computer Crimes
DATE:	April 24, 2014 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Telotte/Walsh	Caldwell	CU	**Fav/CS**
2.	Cellon	Cannon	CJ	**Fav/CS**
3.	Clodfelter	Sadberry	ACJ	**Fav/CS**
4.	Clodfelter	Kynoch	AP	**Fav/CS**

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

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

Three crimes are added to "offenses against users of computer networks and electronic devices"[1] 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 without authorization[2];
- 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;[3] and

[1] s. 815.06, F.S.
[2] Punishable as a third degree felony which could result in 5 years imprisonment and a $5,000 fine. ss. 775.082, 775.083, F.S.
[3] A second degree felony punishable by up to 15 years imprisonment and a $15,000 fine. ss. 775.082, 775.083, F.S.

- 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.[4]

"Offenses against public utilities" are created in the bill and two additional crimes are created, 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, a third degree felony; and
- Physically tampering with, inserting a computer contaminant 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, a second degree felony.

The Criminal Justice Impact Conference determined that the previous version of the bill (CS/CS/SB 364) would have an insignificant impact on the need for prison beds; the changes made in CS/CS/CS/SB 364 do not appear to affect that determination.

II. Present Situation:

Offenses against intellectual property

Section 815.04, F.S., provides that 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

Section 815.06, F.S., provides that 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

[4] A first degree felony punishable by up to 30 years imprisonment and a fine of $10,000. ss. 775.082, 775.083, F.S.

- 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." A computer network 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 by the bill 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. The bill includes cellular telephones, tablets, and other portable communications devices as examples of electronic devices. These changes allow for devices other than the standard computer to be considered capable of being used to commit an offense.

Section 3 amends s. 815.04, F.S., to include the term "electronic devices" in the existing definition of offenses against intellectual property. It also creates new offenses of introducing a computer contaminant and rendering data unavailable.

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 the bill is passed during the same legislative session and becomes law.

Section 4 amends s. 815.06, F.S., and renames these offenses "offenses against users of computer networks and electronic devices." It defines the term "user" to mean "a person with the authority to operate or maintain a computer network or electronic device."

The bill creates a new third degree felony where a person willfully, knowingly, and without authorization engages in audio or video surveillance of an individual without the individual's authorization 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.

Additionally, if a person commits an offense against users of computer networks and electronic devices and 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., it is punishable as a second degree felony.

The bill also provides that it is a first degree felony for a person to commit an offense against users of a computer network and electronic devices and disrupt 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.

As amended by the bill, revised s. 815.06, F.S., does not apply to a person who has acted pursuant to a search warrant or to an exception to a search warrant authorized by law or when acting within the scope of his or her employment and authorized security operations of a government or business.

Under s. 815.06, F.S., as amended by the bill, providers of the following services are exempt from liability:

- Interactive computer service;[5]
- Information service;[6]
- Communications services where the provider provides transmission, storage, or caching of electronic communications or messages of others;[7]

[5] As defined in 47 U.S.C. 230(f)(2): The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

[6] The term "information service" means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service. 47 U.S.C. 153(24).

[7] "Communications services" means the transmission, conveyance, or routing of voice, data, audio, video, or any other information or signals, including video services, to a point, or between or among points, by or through any electronic, radio, satellite, cable, optical, microwave, or other medium or method now in existence or hereafter devised, regardless of the protocol used for such transmission or conveyance. The term includes such transmission, conveyance, or routing in which computer processing applications are used to act on the form, code, or protocol of the content for purposes of transmission, conveyance, or routing without regard to whether such service is referred to as voice-over-Internet-protocol services or is classified by the Federal Communications Commission as enhanced or value-added. The term does not include: information services; installation or maintenance of wiring or equipment on a customer's premises; the sale or rental of tangible personal property; the sale of advertising, including, but not limited to, directory advertising; bad check charges; late payment charges; billing and collection services; or internet access service, electronic mail service, electronic bulletin board service, or similar online computer services. s. 202.11, F.S.

- Other related telecommunications or commercial mobile radio service; or
- Content provided by another person.

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 a computer contaminant 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.

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:

CS/CS/CS/SB 364 may provide better protection against economic loss to owners and users of computers, computer systems, and electronic devices as well as the providers of services related to these devices.

C. Government Sector Impact:

The Criminal Justice Impact Conference determined that CS/CS/SB 364 would have an insignificant impact on the need for prison beds; the changes in CS/CS/CS/SB 364 do not appear to affect that determination.

VI. Technical Deficiencies:

None.

VII. Related Issues:

Section 815.06(2)(f), F.S., created in Section 5 of the bill, appears to be intended to prohibit a person from secretly surveilling another person by gaining unauthorized control of cameras or other features of a computer or electronic device that is not their own. However, if the "without authorization" element of the offense is not construed to apply to the act of "accessing any inherent feature or component of a computer," the provision could be interpreted to prevent private property owners from conducting surveillance on and around their property without first obtaining the authorization of any individual who is on the property. Although it is possible that authorization would be inferred from a person's presence in a location, this may not always be the case. For example, signs are posted in many retail establishments to notify persons that they are under surveillance while inside the store or even in the parking lot. Authorization may be inferred from the fact that the business owner gave notification of the surveillance and the customer chose to remain at the business. However, signs are not posted in every place where a person is under surveillance. For example, a homeowner who has a security camera to surveil his property may not post a sign to disclose that fact. If there is no notice to make a person who is on the property aware of the surveillance, it may be difficult to infer authorization simply by the person's presence on the property.

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/CS/CS by Appropriations on April 24, 2014:
The committee substitute:

- Adds a new offense of "inserting a computer contaminant" to existing crimes relating to unauthorized activities concerning computers.
- Includes cellular telephones, tablets, and other portable communications devices as examples of electronic devices.
- Amends s. 815.06, F.S., to replace the bill's new definition of "person" with a definition of "user."
- Adds "authorized security operations of a government or business" to the exceptions created in the bill for activities that would otherwise violate s. 815.05, F.S.
- Makes technical and conforming changes.

CS/CS by Criminal Justice on February 17, 2014:
CS/CS/SB 364 amends s. 815.06, F.S., to exempt the providers of listed services from liability under any construction of the bill. It also requires a person's authorization, rather than knowledge, for audio or video surveillance of the person using the systems and devices listed in 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.