

HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/CS/CS/HB 641 Computer Crimes

SPONSOR(S): Judiciary Committee; Justice Appropriations Subcommittee; Criminal Justice Subcommittee and La Rosa

TIED BILLS: CS/CS/HB 643 **IDEN./SIM. BILLS:** CS/CS/CS/SB 364

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Criminal Justice Subcommittee	11 Y, 0 N, As CS	Jones	Cunningham
2) Justice Appropriations Subcommittee	13 Y, 0 N, As CS	McAuliffe	Lloyd
3) Judiciary Committee	17 Y, 0 N, As CS	Jones	Havlicak

SUMMARY ANALYSIS

Chapter 815, F.S., entitled the "Florida Computer Crimes Act," was created in 1978 in recognition of growing computer-related crime. The chapter establishes legislative intent, and a variety of computer-related offenses and definitions.

The bill adds legislative intent language that recognizes that the proliferation of new technologies impact computer-related crimes. To this end, the bill amends the definition of computer network and creates a definition of the term *electronic device*, which means "a device or a portion of a device that is designed for and capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data, including, but not limited to, a cellular telephone, tablet, or other portable device designed for and capable of communicating with or across a computer network and that is actually used for such purpose."

The bill also:

- Creates new computer-related offenses and expands the application of various existing computer-related crimes to include electronic devices;
- Broadens and creates additional exceptions to computer-related offenses for persons who act pursuant to a search warrant, an exception to a search warrant, or who perform authorized security operations of a government or business;
- Expands the entities that can bring a civil action against persons convicted of computer-related offenses by including owners and lessees of electronic devices;
- Adds electronic devices to the list of items subject to forfeiture if used in computer-related offenses; and
- Provides nothing in this act may be construed to impose liability on certain computer service providers.

The bill also creates new second and third degree felony offenses relating to public utilities.

On March 3, 2014, the Criminal Justice Impact Conference determined that the bill will have an insignificant negative prison bed impact on the Department of Corrections.

The bill is effective October 1, 2014.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

The Florida Computer Crime Act

Chapter 815, F.S., entitled the “Florida Computer Crimes Act,” was created in 1978¹ in recognition of growing computer-related crime. The chapter establishes legislative intent, and a variety of computer-related offenses and definitions.

Legislative Intent

Currently, s. 815.02, F.S., provides that the Legislature finds and declares that:

- Computer-related crime is a growing problem in government as well as in the private sector;
- Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime;
- The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great; and
- While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.

Effect of the Bill

The bill amends s. 815.02, F.S., to add additional legislative intent language, which states that:

- 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.

Definitions

Section 815.03, F.S., provides numerous definitions that apply to ch. 815, F.S. For example, s. 815.03(3), F.S., defines *computer contaminant* as “any set of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. The term includes, but is not limited to, a group of computer instructions, commonly called viruses or worms, which are self-replicating or self-propagating and which are designed to contaminate other computer programs or computer data; consume computer resources; modify, destroy, record, or transmit data; or in some other fashion usurp the normal operation of the computer, computer system, or computer network.”

A *computer network* is also defined as “any system that provides communications between one or more computer systems and its input or output devices, including, but not limited to, display terminals and printers that are connected by telecommunication facilities.”

Effect of the Bill

The bill amends the definition of a *computer contaminant* to include *interfering* with the normal operation of the computer, computer system, or computer network.

The bill also amends the definition of *computer network* to mean “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 systems or electronic devices by physical or wireless telecommunication facilities.”

¹ Chapter 78-92, L.O.F.
STORAGE NAME: h0641e.JDC
DATE: 3/31/2014

The bill creates a definition of the term *electronic device*, which means “a device or a portion of a device that is designed for and capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data, including, but not limited to, a cellular telephone, tablet, or other portable device designed for and capable of communicating with or across a computer network and that is actually used for such purpose.”

Offenses Against Intellectual Property

Section 815.04, F.S., makes it a third degree felony² for a person to:

- Willfully, knowingly, and without authorization modify data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network;
- Willfully, knowingly, and without authorization destroy 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 secret³ or is confidential that is residing or existing internal or external to a computer, computer system, or computer network.

It is a second degree felony⁴ if any of the above offenses are committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property.

Effect of the Bill

The bill expands the application of s. 815.04, F.S., by prohibiting a person from:

- *Introducing a computer contaminant* or modifying or *rendering unavailable* or destroying data, etc. located on a computer, computer system, computer network, or an *electronic device*; and
- Disclosing or taking data, programs, or supporting documents which is a trade secret or is confidential that is residing or existing internal or external to a computer, computer system, computer network, or an *electronic device*.

Offenses Against Computer Users

Criminal Penalties

Section 815.06(1), F.S., makes it a third degree felony for a person to willfully, knowingly, and without authorization:

- (a) Access or cause to be accessed any computer, computer system, or computer network;
- (b) Disrupt or deny or cause the denial of computer system services to an authorized user of a 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;
- (c) Destroy, take, injure, or damage equipment or supplies used or intended to be used in a computer, computer system, or computer network;
- (d) Destroy, injure, or damage any computer, computer system, or computer network; or
- (e) Introduce any computer contaminant into any computer, computer system, or computer network.

It is a second degree felony if a person violates subsection (1) and the person:

- Damages a computer, computer equipment, computer supplies, 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;
- Commits the offense for the purpose of devising or executing any scheme or artifice to defraud or obtain property; or

² A third degree felony is punishable by up to five years imprisonment and a \$5,000 fine. Sections 775.082 and 775.083, F.S.

³ Section 812.081, F.S., defines a “trade secret” as the whole or any portion or phase of any formula, pattern, device, combination of devices, or compilation of information which is for use, or is used, in the operation of a business and which provides the business an advantage, or an opportunity to obtain an advantage, over those who do not know or use it. “Trade secret” includes any scientific, technical, or commercial information, including any design, process, procedure, list of suppliers, list of customers, business code, or improvement thereof. Irrespective of novelty, invention, patentability, the state of the prior art, and the level of skill in the business, art, or field to which the subject matter pertains, a trade secret is considered to be: a Secret; Of value; For use or in use by the business; and Of advantage to the business, or providing an opportunity to obtain an advantage, over those who do not know or use it.

⁴ A second degree felony is punishable by up to 15 years imprisonment and a \$10,000 fine. Sections 775.082 and 775.083, F.S.

- Interrupts or impairs a governmental operation or public communication, transportation, or supply of water, gas, or other public service.⁵

It is a first degree felony⁶ if a person violates subsection (1) and the violation endangers human life.⁷ Section 815.06(3), F.S., makes it a first degree misdemeanor⁸ for a person to willfully, knowingly, and without authorization modify equipment or supplies used or intended to be used in a computer, computer system, or computer network.

None of the criminal penalties apply to a person who accesses his or her employer's computer system, computer network, computer program, or computer data when acting within the scope of his or her lawful employment.⁹

Civil Remedies and Forfeiture

Currently, the owner or lessee of the computer, computer system, computer network, computer program, computer equipment, computer supplies, or computer data is authorized to bring a civil action against any person convicted under s. 815.06, F.S., for compensatory damages.¹⁰ In such actions, the court may award reasonable attorney's fees to the prevailing party.¹¹

For purpose of determining where a civil (or criminal) action may be brought, s. 816.06(7), F.S., specifies that in instances where a person causes the access to a computer, computer system, or computer network in one jurisdiction from another jurisdiction, the person is deemed to have personally accessed the computer, computer system, or computer network in both jurisdictions.

Additionally, any computer, computer system, computer network, computer software, or computer data owned by a defendant which is used during the commission of any violation s. 815.06, F.S., or any computer owned by a defendant which is used as a repository for the storage of software or data obtained in violation of s. 815.06, F.S., is subject to forfeiture as provided under ss. 932.701-932.704, F.S.¹²

Effect of the Bill

Criminal Penalties

The bill renames offenses against computer users to offenses against users of computers, computer systems, computer networks and electronic devices. The bill renumbers s. 815.06(1), F.S., to s. 815.06(2), F.S., and expands the application of the statute to include electronic devices and to include additional prohibited acts. Specifically, the bill:

- Amends paragraph (a) to prohibit a person from accessing, or causing to be accessed, any computer, computer system, computer network, *or electronic device*, with knowledge that the access is unauthorized;
- Amends paragraph (b) to prohibit a person from disrupting or denying or causing the denial of *the ability to transmit data to or from* an authorized user of a *computer, computer system computer network or computer network services*;
- Amends paragraphs (c) and (d) to include *electronic devices* in the list of property a person is prohibited from destroying, taking, injuring, or damaging;
- Amends paragraph (e) to include *electronic devices* in the list of property a person is prohibited from introducing contaminants into; and
- Creates paragraph (f) which prohibits a person from willfully, knowingly, and without authorization engaging in audio or video surveillance of an individual by accessing any inherent feature or component of a computer, computer system, computer network, or electronic device,

⁵ Section 815.06(2)(b), F.S.

⁶ A first degree felony is punishable by up to 30 years imprisonment and a \$10,000 fine. Sections 775.082 and 775.083, F.S.

⁷ Section 815.06(2)(c), F.S.

⁸ A first degree misdemeanor is punishable by up to one year in county jail and a \$1,000 fine. Sections 775.082 and 775.083, F.S.

⁹ Section 815.06(6), F.S.

¹⁰ Section 815.06(4), F.S.

¹¹ *Id.*

¹² Section 815.06(5), F.S.

including accessing the data or information of a computer, computer system, computer network, or electronic device that is stored by a third party.

The bill also expands the instances in which the penalty for violating s. 815.06, F.S., is increased to a second degree felony. Specifically, the bill makes it a second degree felony if a person commits any of the above-described acts and the person:

- 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.

The bill also adds another instance in which the penalty for violating s. 815.06, F.S., is increased to a first degree felony. Specifically, the bill makes it a first degree felony if a person commits any of the above-described acts and the violation 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 broadens the application of the misdemeanor offense by prohibiting persons from modifying equipment or supplies used or intended to be used in a computer, computer system, computer network, or *electronic device*.

The bill broadens the current exception by specifying that the offenses in s. 815.06, F.S., do not apply to a person who accesses his or her employer's computer system, computer network, computer program, computer data, or *electronic device* when acting within the scope of his or her lawful employment. The bill also creates additional exceptions for persons who;

- Acts pursuant to a search warrant, an exception to a search warrant; or
- Performs authorized security operations of a government or business.

The bill defines the term "user" as a person with the authority to operate or maintain a computer, computer system, computer network, or electronic device.

The bill provides that nothing in this act may be construed to impose liability on any provider of an interactive computer service, as defined in 47 U.S.C. 230(f); information service, as defined in 47 U.S.C. 153; or communications service as defined in s. 202.11, F.S., when the provider provides the transmission, storage or caching of electronic communications or messages of others; other related telecommunications or commercial mobile radio service; or content provided by another person.

Civil Remedies and Forfeiture

The bill expands the entities that can bring a civil action against persons convicted of s. 815.06, F.S., by including owners and lessees of *electronic devices*.

For purpose of determining where a civil (or criminal) action may be brought, the bill specifies that in instances where a person causes the access to a computer, computer system, computer network, or *electronic device* in one jurisdiction from another jurisdiction, the person is deemed to have personally accessed the computer, computer system, computer network, or *electronic device* in both jurisdictions. The bill adds *electronic devices* to the list of items subject to forfeiture if used in a violation of s. 815.06, F.S.

The bill makes conforming changes to the offense severity ranking chart in s. 921.0022, F.S.

Offenses Against Public Utilities

Currently, ch. 815, F.S., does not include any offenses relating to public utilities.

Effect of the Bill

The bill creates s. 815.061, F.S., to make it a third degree felony for a person to willfully, knowingly, and without authorization gain 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.

The bill makes it a second degree felony for a person to 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 cause a disruption in any service delivered by a public utility.

The bill defines term *public utility*, to include:

- A public utility or electric utility as defined in s. 366.02, F.S.;
- A utility as defined in s. 367.021, F.S.;
- A natural gas transmission company as defined in s. 368.103, F.S.;
- A 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
- A 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

B. SECTION DIRECTORY:

Section 1. Amends s. 721.071, F.S., relating to trade secrets.

Section 2. Amends s. 815.02, F.S., relating to legislative intent.

Section 3. Amends s. 815.03, F.S., relating to definitions.

Section 4. Amends s. 815.04, F.S., relating to offenses against intellectual property; public records exemption.

Section 5. Amends s. 815.06, F.S., relating to offenses against computer users.

Section 6. Creates s. 815.061, F.S., relating to offenses against public utilities.

Section 7. Amends s. 921.0022, F.S., relating to Criminal Punishment Code; offense severity ranking chart.

Section 8. Provides an effective date of October 1, 2014.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

The bill does not appear to have any impact on state revenues.

2. Expenditures:

On March 3, 2014, the Criminal Justice Impact Conference determined that the bill will have an insignificant negative prison bed impact on the Department of Corrections.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

The bill does not appear to have any impact on local government revenues.

2. Expenditures:

The bill may have a negative jail bed impact in that it broadens the application of the first degree misdemeanor offense in s. 815.06, F.S.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

The bill appears to be exempt from the requirements of Article VII, Section 18 of the Florida Constitution because it is a criminal law.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

The bill does not appear to create the need for rulemaking or rulemaking authority.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On February 12, 2014, the Criminal Justice Subcommittee adopted one amendment and reported the bill favorable as a committee substitute. The amendment:

- Corrected terminology;
- Expanded the application of s. 815.04(3), F.S., by prohibiting a person from disclosing or taking certain data located on an *electronic device*;
- Expanded the definition of the term "public utility; and
- Amended the Criminal Punishment Code severity ranking chart for purposes of incorporating the changes made to s. 815.04, F.S.

On March 11, 2014, the Justice Appropriations Subcommittee adopted one amendment and reported the bill favorable as a committee substitute. The amendment provides that nothing in this act may be construed to impose liability on certain computer service providers.

On March 27, 2014, the Judiciary Committee adopted one amendment and reported the bill favorable as a committee substitute. The amendment:

- Refines the definition of electronic device to include such devices as cell phones and tablets;
- Adds *interfering* with the normal operation of the computer, computer system, or computer network, to the definition of a computer contaminant;
- Adds introduction of a computer contaminant in the offenses against intellectual property;
- Renames offenses against computer users to offenses against users of computers, computer systems, computer networks and electronic devices;
- Adds the definition of "user" to offenses against users of computers, computer systems, computer networks and electronic devices;

- Broadens the current exception and adds additional exceptions to offenses against users of computers, computer systems, computer networks and electronic devices; and
- Clarifies that it is an offense against public utilities to insert a *computer contaminant* into a computer, computer system, computer network or electronic device.

This analysis is drafted to the committee substitute as passed by the Judiciary Committee.