FLORIDA COMPUTER CRIMES ACT

815.01 Short title.--The provisions of this act shall be known and may be cited as the "Florida Computer Crimes Act."

History.--s. 1, ch. 78-92.

815.02 Legislative intent.--The Legislature finds and declares that:

(1) Computer-related crime is a growing problem in government as well as in the private sector.

(2) 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.

(3) 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.

(4) 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.

History.--s. 1, ch. 78-92.

815.03 Definitions.--As used in this chapter, unless the context clearly indicates otherwise:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

(2) "Computer" means an internally programmed, automatic device that performs data processing.

(3) "Computer contaminant" means 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.

(4) "Computer network" means 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.

(5) "Computer program or computer software" means a set of instructions or statements and related data which, when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(6) "Computer services" include, but are not limited to, computer time; data processing or storage functions; or other uses of a computer, computer system, or computer network.

(7) "Computer system" means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files.

(8) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs, or instructions. Data may be in any form, in storage media or stored in the memory of the computer, or in transit or presented on a display device.

(9) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

(10) "Intellectual property" means data, including programs.

(11) "Property" means anything of value as defined in 1s. 812.011 and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine-readable or human-readable form, and any other tangible or intangible item of value.

History.--s. 1, ch. 78-92; s. 9, ch. 2001-54.

1Note.--Repealed by s. 16, ch. 77-342.

815.04 Offenses against intellectual property; public records exemption.--

(1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(3)(a) Data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 which resides or exists internal or external to a computer, computer system, or computer network which is held by an agency as defined in chapter 119 is confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

(b) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(4)(a) Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

History.--s. 1, ch. 78-92; s. 1, ch. 94-100; s. 431, ch. 96-406.

815.045 Trade secret information.--The Legislature finds that it is a public necessity that trade secret information as defined in s. 812.081, and as provided for in s. 815.04(3), be expressly made confidential and exempt from the public records law because it is a felony to disclose such records. Due to the legal uncertainty as to whether a public employee would be protected from a felony conviction if otherwise complying with chapter 119, and with s. 24(a), Art. I of the State Constitution, it is imperative that a public records exemption be created. The Legislature in making disclosure of trade secrets a crime has clearly established the importance attached to trade secret protection. Disclosing trade secrets in an agency's possession would negatively impact the business interests of those providing an agency such trade secrets by damaging them in the marketplace, and those entities and individuals disclosing such trade secrets would hesitate to cooperate with that agency, which would impair the effective and efficient administration of governmental functions. Thus, the public and private harm in disclosing trade secrets significantly outweighs any public benefit derived from disclosure, and the public's ability to scrutinize and monitor agency action is not diminished by nondisclosure of trade secrets.

History.--s. 2, ch. 94-100.

Note.--Former s. 119.165.

815.06 Offenses against computer users.--

(1) Whoever willfully, knowingly, and without authorization:

(a) Accesses or causes to be accessed any computer, computer system, or computer network;

(b) Disrupts or denies or causes the 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;

(c) Destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network;

(d) Destroys, injures, or damages any computer, computer system, or computer network; or

(e) Introduces any computer contaminant into any computer, computer system, or computer network,

commits an offense against computer users.

(2)(a) Except as provided in paragraphs (b) and (c), whoever violates subsection (1) commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) Whoever violates subsection (1) and:

1. 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;

2. Commits the offense for the purpose of devising or executing any scheme or artifice to defraud or obtain property; or

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

commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(c) Whoever violates subsection (1) and the violation endangers human life commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(3) Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

(4)(a) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, computer equipment, computer supplies, or computer data may bring a civil action against any person convicted under this section for compensatory damages.

(b) In any action brought under this subsection, the court may award reasonable attorney's fees to the prevailing party.

(5) Any computer, computer system, computer network, computer software, or computer data owned by a defendant which is used during the commission of any violation of this section or any computer owned by the defendant which is used as a repository for the storage of software or data obtained in violation of this section is subject to forfeiture as provided under ss. 932.701-932.704.

(6) This section does not apply to any 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.

(7) For purposes of bringing a civil or criminal action under this section, a person who causes, by any means, the access to a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in both jurisdictions.

History.--s. 1, ch. 78-92; s. 11, ch. 2001-54.

815.07 This chapter not exclusive.--The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter.