UIC John Marshall Journal of Information Technology & Privacy Law

Volume 2
Issue 1 *Computer/Law Journal - 1980*

Article 24

1980

Current and Proposed Computer Crime Legislation, 2 Computer L.J. 721 (1980)

Michael M. Krieger

CURRENT AND PROPOSED COMPUTER CRIME LEGISLATION

Compiled by MICHAEL M. KRIEGER*

TABLE OF CONTENTS

* Ph.D. 1969 in mathematics and J.D. 1980, University of California at Los Angeles. Dr. Krieger was on the mathematics faculty at U.C.L.A. and the Massachusetts Institute of Technology prior to entering law school. He has continued to do research and consulting in the area of communications networks, in addition to legal areas relating to technology. He is currently a Fellow of the National Center for Computer Crime Data.

I. FEDERAL LEGISLATION (PROPOSED)

F-1 S. 240 (1979) (showing amendments from S. 1766 (1977))[1]

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Computer Systems Protection Act of 1979".

SEC. 2. The Congress finds that—

(1) computer-related crime is a growing problem in the Government and in the private sector;

(2) such 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 Federal programs, in financial institutions, and in other entities which operate in interstate commerce through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets, are great;

(4) computer-related crime directed at institutions operating in interstate commerce has a direct effect on interstate commerce; and

(5) the prosecution of persons engaged in computer-related crime is difficult under current Federal criminal statutes.

SEC. 3.(a) Chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following new section:

§ 1028. Computer fraud and abuse

(a) Whoever knowingly and willfully, directly or indirectly accesses, causes to be accessed or attempts to access any computer, computer system, computer network, or any part thereof which, in whole or in part, operates in interstate commerce or is owned by, under contract to, [or operated for, or on behalf of] or in conjunction with, any financial institution, the United States Government or any

1. Those amendments made by S. 1766 are shown by using underlining for deletions from S. 240 as original introduced, and bracketed text for additions.

branch, department, or agency thereof, or any entity operating in or affecting interstate commerce, for the purpose of—

(1) devising or executing any scheme or artifice to defraud, or

(2) obtaining money, property, or service, for themselves or another, by means of false or fraudulent pretenses, representations or promises, shall be fined a sum not more than [$50,000] two and one-half times the amount of the fraud or theft, or imprisoned not more than fifteen years, or both.

(b) Whoever intentionally and without authorization, directly or indirectly accesses, alters, damages, destroys, or attempts to damage or destroy any computer, computer system, or computer network described in subsection (a), or any computer software, program or data contained in such computer, computer system or computer network, shall be fined not more than $50,000 or imprisoned not more than fifteen years, or both.

(c) For purposes of this section, the term—

(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 electronic device which performs logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network;

(3) "computer system" means a set of related, connected or unconnected, computer equipment, devices, and software;

(4) "computer network" means the interconnection of communication [lines] systems with a computer through remote terminals, or a complex consisting of two or more interconnected computers;

(5) "property" includes, but is not limited to, financial instruments, information, including electronically processed or produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value;

(6) "services" includes, but is not limited to, computer time, data processing, and storage functions;

(7) "financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange,

credit card, or marketable security, or any electronic data processing representation thereof;

(8) "computer program" means an instruction or statement or a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system;

(9) "computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system;

(10) "financial institution" means—

(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

(B) a member of the Federal Reserve including any Federal Reserve bank;

(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

(D) a credit union with accounts insured by the National Credit Union Administration;

(E) a member of the Federal home loan bank systems and any home loan bank;

(F) a member or business insured by the Securities Investor Protection Corporation; and

(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934.

F-2 S. 240 (1980) (revision proposed in Committee)

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Computer Systems Protection Act of 1979".

SEC. 2. The Congress finds that—

(1) computer-related crime is a growing problem in the Government and in the private sector;

(2) such 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 Federal programs, in financial institutions, and in computers which operate in or use a facility of interstate commerce through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets, are great;

(4) computer-related crime directed at computers which operate in or use a facility of interstate commerce has a direct effect on interstate commerce; and

(5) the prosecution of persons engaged in computer-related crime is difficult under current Federal criminal statutes.

SEC. 3. (a) Chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following new section:

"§ 1028. Computer fraud and abuse

"(a) Whoever uses, or attempts to use, a computer with intent to execute a scheme or artifice to defraud, or to obtain property by false or fraudulent pretenses, representations, or promises, or to embezzle, steal, or knowingly convert to his use or the use of another, the property of another, shall, if the computer—

"(1) is owned by, under contract to, or operated for or on behalf of:

"(A) the United States Government; or

"(B) a financial institution;

and the prohibited conduct directly involves or affects the computer operation for or on behalf of the United States Government or financial institution; or

"(2) operates in, or uses a facility of, interstate commerce;

be fined not more than two times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned not more than five years, or both.

"(b) Whoever intentionally and without authorization damages a computer described in subsection (a) shall be fined not more than $50,000 or imprisoned not more than five years or both.

"(c) DEFINITIONS.—For the purpose of this section, the term—

"(1) 'computer' means a device that performs logical, arithmetic, and storage functions by electronic manipulation, and includes any property and communication facility directly related to or operating in conjunction with such a device; but does not include an automated typewriter or typesetter, or any computer designed and manufactured for, and which is used exclusively

for routine personal, family, or household purposes including a portable hand-held electronic calculator;

"(2) 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Corporation;

"(B) a member of the Federal Reserve including any Federal Reserve bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank systems any home loan bank;

"(F) a member or business insured by the Securities Investor Protection Corporation; and

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934;

"(3) 'property' means anything of value, and includes tangible and intangible personal property, information in the form of electronically processed, produced, or stored data, or any electronic data processing representation thereof, and services;

"(4) 'services' includes computer data processing and storage functions;

"(5) 'United States Government' includes a branch or agency thereof; and

"(6) 'use' includes to instruct, communicate with, store data in, or retrieve data from, or otherwise utilize the logical, arithmetic, or memory functions of a computer.

"(d)(1) In a case in which Federal jurisdiction over an offense as described in this section exists concurrently with State or local jurisdiction, the existence of Federal jurisdiction does not, in itself, require the exercise of Federal jurisdiction, nor does the initial exercise of Federal jurisdiction preclude its discontinuation.

"(2) In a case in which Federal jurisdiction over an offense as described in this section exists or may exist concurrently with State or local jurisdiction, Federal law enforcement officers, in determining whether to exercise jurisdiction, should consider—

"(A) the relative gravity of the Federal offense and the State or local offense;

"(B) the relative interest in Federal investigation or prosecution;

"(C) the resources available to the Federal authorities and the State or local authorities;

"(D) the traditional role of the Federal authorities and the State or local authorities with respect to the offense;

"(E) the interests of federalism; and

"(F) any other relevant factor.

"(3) The Attorney General shall—

"(A) consult periodically with representatives of State and local governments concerning the exercise of jurisdiction in case in which Federal jurisdiction as described in this section exists or may exist concurrently with State or local jurisdiction;

"(B) provide general direction to Federal law enforcement officers concerning the appropriate exercise of such Federal jurisdiction;

"(C) report annually to Congress concerning the extent of the exercise of such Federal jurisdiction during the preceding fiscal year; and

"(D) report to Congress, within one year of the effective date of this Act, on the long-term impact upon Federal jurisdiction, of this Act and, the increasingly pervasive and widespread use of computers in the United States. The Attorney General shall periodically review and update such report.

"(4) Except as otherwise prohibited by law, information or material obtained pursuant to the exercise of Federal jurisdiction may be made available to State or local law enforcement officers having concurrent jurisdiction, and to State or local authorities otherwise assigned responsibility with regard to the conduct constituting the offense.

"(5) An issue relating to the propriety of the exercise of, or of the failure to exercise, Federal jurisdiction over an offense as described in this section, or otherwise relating to the compliance, or to the failure to comply, with this section, may not be litigated, and a court may not entertain or resolve such an issue except as may be necessary in the course of granting leave to file a dismissal of an indictment, an information, or a complaint.".

II. STATE STATUTES ENACTED

S-1 Arizona

TITLE 13, CRIMINAL CODE (Ariz. Rev. Stat. Anno.) (West)

§ 13-2301 Definitions.

* * *

E. For the purposes of § 13-2316:

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 electronic device which performs logic, arithmetic or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network.

3. "Computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of two or more interconnected computers.

4. "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system.

5. "Computer software" means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

6. "Computer system" means a set of related, connected or unconnected computer equipment, devices and software.

7. "Financial instrument" means any check, draft, money order, certificate of desposit, letter of credit, bill of exchange, credit card, marketable security or any other written instrument, as defined by § 18-2001, paragraph 7, which is transferable for value.

8. "Property" means financial instruments, information, including electronically produced data, computer software and programs in either machine or human readable form, and anything of value, tangible or intangible.

9. "Services" includes computer time, data processing and storage functions.

§ 13-2316. Computer fraud; classification.

A. A person commits computer fraud in the first degree by accessing, altering, damaging or destroying without authorization any computer, computer system, computer network, or any part of such

computer, system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or control property or services by means of false or fraudulent pretenses, representations or promises.

B. A person commits computer fraud in the second degree by intentionally and without authorization accessing, altering, damaging or destroying any computer, computer system or computer network or any computer software, program or data contained in such computer, computer system or computer network.

C. Computer fraud in the first degree is a class 3 felony. Computer fraud in the second degree is a class 6 felony.

S-2 California

CAL. PENAL CODE (1980 Supp.) (West)

§ 502. Definitions; computer system or network; Intentional access to defraud or extort, or to obtain money, property or services with false or fraudulent intent, representation or promises, malicious access, alteration, deletion or damage; violations, penalty

(a) For purposes of this section:

(1) "Access" means to instruct, communicate with, store data in, or retrieve data from a computer system or computer network.

(2) "Computer system" means a machine or collection of machines, excluding pocket calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs and data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(3) "Computer network" means an interconnection of two or more computer systems.

(4) "Computer program" means an ordered set of instructions or statements and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.

(5) "Data" means a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner, and are intended for use in a computer system or computer network.

(6) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authoriza-

tion mechanism, marketable security, or any computer system representation thereof.

(7) "Property" includes, but is not limited to, financial instruments, data, computer programs, documents associated with computer systems and computer programs, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit.

(8) "Services" includes, but is not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data contained within a computer system, or data contained within a computer network.

(b) Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises shall be guilty of a public offense.

(c) Any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense.

(d) Any person who violates the provisions of subdivision (b) or (c) is guilty of a felony and is punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.

(e) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction.

S-3 Colorado

CRIMINAL JUSTICE CODE (Colo. Rev. Stat.) (1979 Supp.)

18-5.5-101. Definitions.

As used in this article, unless the context otherwise requires:

(1) To "use" means to 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 electronic device which performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output,

processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.

(3) "Computer network" means the interconnection of communication lines (including microwave or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(4) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system.

(5) "Computer software" means computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software.

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

(8) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(9) "Service" includes, but is not limited to, computer time, data processing, and storage functions.

18-5.5-102. Computer crime.

(1) Any person who knowingly uses any computer, computer system, computer network, or any part thereof for the purpose of: Devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; or commiting theft commits computer crime.

(2) Any person who knowingly and without authorization uses, alters, damages, or destroys any computer, computer system, or computer network described in section 18-5.5-101 or any computer software, program, documentation, or data contained in such computer, computer system, or computer network commits computer crime.

(3) If the loss, damage, or thing of value taken in violation of this section is less than fifty dollars, computer crime is a class 3 misdemeanor; if fifty dollars or more but less than two hundred dollars, computer crime is a class 2 misdemeanor; if two hundred dollars or

more but less than ten thousand dollars, computer crime is a class 4 felony; if ten thousand dollars or more, computes crime in a class 3 felony.

S-4 Florida

FLA. STAT. ANN. §§ 815.01-815.07 (West Supp.).

815.01 Short title

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

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.

815.03 Definitions

As used in this chapter, unless the context clearly indicates otherwise:

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

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

(4) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(5) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, or computer software.

(6) "Computer network" means a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.

(7) "Computer system services" means providing a computer system or computer network to perform useful work.

(8) "Property" means anything of value as defined in s. 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.

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

(10) "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.

815.04 Offenses against intellectual property

(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) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in § 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 § 775.082, § 775.083, or § 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 § 775.082, § 775.083, or § 775.084.

815.05 Offenses against computer equipment or supplies

(1)(a) 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 an offense against computer equipment or supplies.

(b) 1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

2. 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 third degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

(2)(a) Whoever wilfully, knowingly, and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization destroys, injures, or damages any computer, computer system, or computer network commits an offense against computer equipment or supplies.

(b) 1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

2. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is greater than $200 but less than $1,000, then the offender is guilty of a felony of the third degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

3. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is $1,000 or greater, or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service, then the offender is guilty of a felony of the second degree, punishable as provided in § 775.082, § 775.083, or § 775.084

815.06 Offenses against computer users

(1) Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization 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 be-

half of, or in conjunction with another commits an offense against computer users.

(2)(a) Except as provided in this subsection, an offense against computer users is a felony of the third degree, punishable as provided in § 775.082, § 775.083, or § 775.084.

(b) If the offense is committed for the purposes 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 § 775.082, § 775.083, or § 775.084.

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.

S-5 Illinois

ILL. CRIMINAL CODE

Sec. 15-1. Property. As used in this Part C, "property" means anything of value. Property includes * * * computer programs or data * * *.

Sec. 16-9. Unlawful use of computer. (a) As used in this Part C:

1. "Computer" means an internally programmed, general purpose digital device capable of automatically accepting data, processing data and supplying the results of the operation.

2. "Computer system" means a set of related, connected devices, including a computer and other devices, including but not limited to data input and output and storage devices, data communications links, and computer programs and data, that make the system capable of performing the special purpose data processing tasks for which it is specified.

3. "Computer program" means a series of coded instructions or statements in a form acceptable to a computer, which causes the computer to process data in order to achieve a certain result.

(b) A person commits unlawful use of a computer when he:

1. Knowingly obtains the use of a computer system, or any part thereof, without the consent of the owner (as defined in Section 15-2); or

2. Knowingly alters or destroys computer programs or data without the consent of the owner (as defined in Section 15-2); or

3. Knowingly obtains use of, alters or destroys a computer system, or any part thereof, as part of a deception for the purpose of obtaining money, property or services from the owner of a computer system (as defined in Section 15-2) or any third party.

(c) Sentence:

1. A person convicted of a violation of subsections (b) (1) or (2) of this Section where the value of the use, alteration, or destruction is $1,000 or less shall be guilty of a petty offense.

2. A person convicted of a violation of subsections (b) (1) or (2) of this Section where the value of the use, alteration or destruction is more than $1,000 shall be guilty of a Class A misdemeanor.

3. A person convicted of a violation of subsection (b) (3) of this Section where the value of the money, property or services obtained is $1,000 or less shall be guilty of a Class A misdemeanor.

4. A person convicted of a violation of subsection (b)(3) of this Section where the value of the money, property or services obtained is more than $1,000 shall be guilty of a Class 4 felony.

(d) This Section shall neither enlarge nor diminish the rights of parties in civil litigation.

S-6 Michigan

MICH. STAT. ANNO. (Callaghan)

§ 28.529(1) Meanings of terms.

SEC. 1. For the purposes of this act, the words and phrases defined in sections 2 and 3 have the meanings ascribed to them in those sections.

§ 28.529(2) Definitions.

SEC. 2. (1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise use the resources of, a computer, a computer system, or computer network.

(2) "Computer" means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes input, output, processing, storage, software, or communication facilities which are connected or related to a device in a system or network.

(3) "Computer network" means the interconnection of communication lines with a computer through remote terminals, or a complex consisting of 2 or more interconnected computers.

(4) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from the computer system.

(5) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software.

§ 28.529(3) Property, services, definitions.

SEC. 3. (1) "Property" includes financial instruments; information, including electronically produced data; computer software and programs in either machine or human readable form; and any other tangible or intangible item of value.

(2) "Services" includes computer time, data processing, and storage functions.

§ 28.529(4) Access to computers, systems or networks, fraudulent purposes, prohibition.

SEC 4. A person shall not, for the purpose of devising or executing a scheme or artifice with intent to defraud or for the purpose of obtaining money, property, or a service by means of a false or fraudulent pretense, representation, or promise with intent to, gain access to or cause access to be made to a computer, computer system, or computer network.

§ 28.529(5) Alteration, damage or destruction, computer, system or network, computer software program or data, prohibition.

SEC. 5. A person shall not intentionally and without authorization, gain access to, alter, damage, or destroy a computer, computer system, or computer network, or gain access to, alter, damage, or destroy a computer software program or data contained in a computer, computer system, or computer network.

§ 28.529(6) Other prohibited acts, violations.

SEC. 6. A person shall not utilize a computer, computer system, or computer network to commit a violation of section 174 of Act No. 328 of the Public Acts of 1934, as amended, being section 750.174 of the Michigan Compiled Laws, section 279 of Act No. 328 of the Public Acts of 1934, being section 750.279 of the Michigan Compiled Laws, section 356 of Act No. 328 of the Public Acts of 1934, as amended, be-

ing section 750.356 of the Michigan Compiled Laws, or section 362 of Act No. 328 of the Public Acts of 1934, as amended, being section 750.362 of the Michigan Compiled Laws.

§ 28.529(7) Violations of act, penalties.

SEC. 7. A person who violates this act, if the violation involves $100.00 or less, is guilty of a misdemeanor. If the violation involves more than $100.00, the person is guilty of a felony, punishable by imprisonment for not more than 10 years, or a fine of not more than $5,000.00, or both.

S-7 New Mexico

CRIMINAL OFFENSES (N. Mex. Stat. Anno.)

30-16A-1. Short title.

This act may be cited as the "Computer Crimes Act."

30-16A-2. Definitions.

As used in the Computer Crimes Act:

A. "access" means to make use of any resources of a computer, computer system or computer network;

B. "computer" means an electronic device which performs logical, arithmetic and memory functions by the manipulation of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a computer system or computer network;

C. "computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of two or more computers and includes interconnected remote terminals;

D. "computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system;

E. "computer software" means a set of computer programs, procedures and associated documentation concerned with the operation and function of a computer system; and

F. "computer system" means a set of related or interconnected computer equipment, devices and software.

30-16A-3. Computer fraud.

A. Any person who accesses or causes to be accessed any computer, computer system, computer network or any part thereof with the intent to devise or execute any scheme or artifice to defraud is guilty of a fourth degree felony. B. Any person who accesses or causes to be accessed any computer, computer system, computer network or any part thereof with the intent to obtain, by means of embezzlement or false or fraudulent pretenses, representation or promises, money, property or services where:

(1) the money, property or services have a value of one hundred dollars ($100) or less, is guilty of a petty misdemeanor;

(2) the money, property or services have a value of one hundred dollars ($100) but not more than two thousand five hundred dollars ($2,500), is guilty of a fourth degree felony; or

(3) the money, property or services have a value of more than two thousand five hundred dollars ($2,500), is guilty of a third degree felony.

30-16A-4. Unauthorized computer use.

Any person who intentionally, maliciously and without authorization accesses, alters, damages or destroys any computer, computer system, computer network, any part thereof or any information stored wherein when:

A. the computer, computer system, computer network, part or information has a value of one hundred dollars ($100) or less is guilty of a petty misdemeanor;

B. the computer, computer system, computer network, part or information has a value of more than one hundred dollars ($100) but not more than two thousand five hundred dollars ($2,500) is guilty of a fourth degree felony; of

C. the computer, computer system, computer network, part or information has a value of more than two thousand five hundred dollars ($2,500) is guilty of a third degree felony.

S-8 North Carolina

N.C. GEN. STAT. (1979 Supp.)

§ 14-453. Definitions.

As used in this section, unless the context clearly requires otherwise, the following terms have the means specified:

(1) "Access" means to approach, instruct, communicate with, cause input, cause output, or otherwise make use of any re-

sources of a computer, computer system or computer network.

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

(3) "Computer network" means the interconnection of communication systems with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(4) "Computer program" means an ordered set of data that are coded instructions or statements that when executed by a computer cause the computer to process data.

(5) "Computer software" means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected computer equipment and devices.

(7) "Financial statement" includes but is not limited to any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card of [or] marketable security, or any electronic data processing representation thereof.

(8) "Property" includes but is not limited to, financial instruments, information, including electronically processed or produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(9) "Services" includes, but is not limited to, computer time, data processing and storage functions.

§ 14-454. Accessing computers.

(a) A person is guilty of a felony if he willfully, directly or indirectly, accesses or causes to be accessed any computer, computer system, computer network, or any part thereof, for the purpose of:

(1) Devising or executing any scheme or artifice to defraud, unless the object of the scheme or artifice is to obtain educational testing material, a false educational testing score, or a false academic or vocational grade, or

(2) Obtaining property or services other than educational testing material, a false educational testing score, or a false academic or vocational grade for himself or another, by means of false or fraudulent pretenses, representations or promises.

(b) Any person who willfully and without authorization, directly or indirectly, accesses or causes to be accessed any computer, computer system, computer network, or any part thereof, for any purpose other than those set forth in subsection (a) above, is guilty of a misdemeanor.

§ 14-455. Damaging computers and related materials.

(a) A person is guilty of a felony if he willfully and without authorization alters, damages or destroys a computer, computer system, computer network, or any part thereof.

(b) A person is guilty of a misdemeanor if he willfully and without authorization alters, damages, or destroys any computer software, program or data residing or existing internal or external to a computer, computer system or computer network.

§ 14-456. Denial of computer services to an authorized user.

Any person who willfully and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, is guilty of a misdemeanor.

§ 14-457. Extortion.

Any person who verbally or by a written or printed communication, maliciously threatens to commit an act described in G.S. 14-450 with the intent to extort money or any pecuniary advantage, or with the intent to compel any person to do or refrain from doing any act against his will, is guilty of a felony.

S-9 Rhode Island

CRIMINAL OFFENSES (1979 Supp.)

11-52-1. Definitions

As used in this chapter:

(A) "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.

(B) "Computer" means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.

(C) "Computer system" means a set of related, connected or unconnected, computer equipment, devices and software.

(D) "Computer network" means the interconnection of communication lines with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(E) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(F) "Services" includes, but is not limited to, computer time, data processing, and storage functions.

(G) "Computer program" means a series of instructions or statements, in a form acceptable to a computer system in a manner designed to provide appropriate products from such computer systems.

(H) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

11-52-2. Access to computer for fraudulent purposes.

Whoever directly or indirectly accesses or causes to be accessed any computer, computer system, or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or (2) obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises shall be guilty of a felony and shall be subject to the penalties set forth in § 11-52-4.

11-52-3. Intentional access, alteration, damage or destruction.

Whoever intentionally and without authorization, directly or indirectly accesses, alters, damages, or destroys any computer, computer system, computer network, computer software, computer program or data contained in such computer, computer system, computer program or computer network shall be guilty of a felony and shall be subject to the penalties set forth in § 11-52-4.

11-52-4. Penalties.

Any person who is convicted of the offenses set forth in §§ 11-52-2 and 11-52-3 shall be fined not more than five thousand dollars ($5,000) or imprisoned for not more than five (5) years, or both.

S-10 Utah

UTAH CRIM. CODE (1979 Supp.)

76-6-701. Computer Fraud Act—Short title.

This act shall be known and may be cited as the "Utah Computer Fraud Act."

76-6-702. Computer Fraud Act—Definitions

As used in this act:

(1) "Access" means to directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of, a computer, computer system, computer network, or any means of communication therewith.

(2) "Computer" means any electronic device or communication facility with data processing ability.

(3) "Computer system" means a set of related, connected or unconnected, devices, software or other related computer equipment.

(4) "Computer network" means the interconnection of communication lines between computers or computers and remote terminals.

(5) "Property" includes, but is not limited to, electronic impulses, electronically produced data, information, financial instruments, software or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and any copies thereof.

(6) "Services" include, but are not limited to, computer time, data manipulation and storage functions.

(7) "Financial instrument" includes, but is not limited to, any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card or marketable security.

(8) "Software" or "program" means a series of instructions or statements in a form acceptable to a computer, relating to the operations of the computer, or permitting the functioning of a computer system in a manner designed to provide results therefrom, including but not limited to, system control programs, application programs, or any copies thereof.

76-6-703. Computer Fraud Act—Offenses—Degree of offense.

Any person who willfully gains access to any computer, computer system, computer network, computer software, computer program or any computer property, who knowingly and willfully provides false information or who causes any other person directly or indirectly to enter false information into any computer, computer system, computer software, computer program, and thereby devises

or executes any scheme or artifice to defraud or obtain money, property, or services including the unauthorized use of computer time, under false pretenses representations, or promises, including representations made to a computer, and thereby alters, damages or destroys any computer, compute system, computer network, computer software, computer program, or computer property, is guilty of a criminal offense, as follows:

(1) For value less than or equal to $25, a class C misdemeanor;

(2) For value greater than $25, but less than or equal to $100, class B misdemeanor;

(3) For value greater than $100, but less than or equal to $300, class A misdemeanor;

(4) For value greater than $300, but less than or equal to $1,000, a felony of the third degree; or

(5) For value greater than $1,000, a felony of the second degree.

76-6-704. Computer Fraud Act—Attorney general—County attorneys—Conduct violating other statutes—Statute of limitations.

(1) The attorney general, with such assistance as he may from time to time request of the county attorneys in the several counties, shall investigate suspected criminal violations of this act and shall commence and try all prosecutions pursuant to this act.

(2) Prosecution pursuant to this act shall not prevent any prosecutions pursuant to any other provision of the law, where such conduct also constitutes a violation of such other provision.

(3) No prosecution may be commenced pursuant to this act more than three years after the commission of the acts constituting a violation of this act.

S-11 Virginia

CODE OF VIRGINIA (1979 Supp.)

§ 18.2-98.1. Computer time, services, etc., subject of larceny.

Computer time or services or data processing services or information or data stored in connection therewith is hereby defined to be property which may be the subject of larceny under § 18.2-95 or 18.2-96, or embezzlement under § 18.2-111, or false pretenses under § 18.2-178.

III. STATE LEGISLATION (PROPOSED)

L-1 Hawaii

S. 504

A Bill For An Act
Relating to Computer Crimes

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

Section 1. The legislature finds that:

(1) Computer-related crime is a growing problem in the government and in the private sector;

(2) Such 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 government programs, in financial institutions, and in other entities through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets, are great; and

(4) The prosecution of persons engaged in computer-related crime is difficult under current state criminal statutes.

Section 2. Chapter 708, Hawaii Revised Statutes, is amended by adding a new section to be appropriately designated and to read:

"Sec. 708-00 Computer fraud. (1) A person commits the offense of computer fraud if the person:

(a) Indirectly or directly, accesses or causes to be accessed any computer, computer system, computer network, or any part thereof for the purposes of:

(i) Devising or executing any scheme or artifice to defraud, or

(ii) Obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises.

(b) Intentionally and without authorization, directly or indirectly, accesses, alters, damages, or destroys any computer, computer system, or computer network, or any computer software, program, or data contained in such computer, computer system, or computer network.

(2) For purposes of this section:

(a) "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;

(b) "Computer" means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network;

(c) "Computer network" means the interconnection of communication lines with a computer through remote terminals, or a complex consisting of two or more interconnected computers;

(d) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system;

(e) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system;

(f) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software;

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

(h) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value; and

(i) "Services" includes, but is not limited to, computer time, data processing, and storage functions.

(3) Computer fraud is a class A felony."

L-2 Maryland

S. 893

AN ACT concerning

Data Processing—Computer Fraud

FOR the purpose of prohibiting fraud by use of a computer; defining

certain terms; establishing penalties; providing a certain exception; and generally relating to fraud by use of a computer.

By redesignating

Article 27—Crimes and Punishments

Subheading "Fraud—Conversion by Factors of Consigned Goods" to apply to Sections 170 through 172 only

Annotated Code of Maryland

(1976 Replacement Volume and 1979 Supplement)

BY adding to

Article 27—Crimes and Punishments

Section 169, 169A, and 169B to be under the new subheading "Fraud—Computer"

Annotated Code of Maryland

(1976 Replacement Volume and 1979 Supplement)

Preamble

WHEREAS, Existing law relative to crimes involving fraud or unauthorized access to or damage or destruction of property does not contain any specific provision relative to computers; and

WHEREAS, While various forms of computer related 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 in the law which proscribes various forms of computer abuse; and

WHEREAS, The prosecution of persons engaged in computer related crime is difficult under current criminal statutes; and

WHEREAS, Computer related crime is a growing problem in government as well as in the private sector; and

WHEREAS, 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; and

WHEREAS, 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

WHEREAS, In recognition of the need to provide a deterrent to fraud by use of a computer, the General Assembly finds and declares that the laws of the State of Maryland shall establish certain unlawful acts and provide for appropriate penalties for persons convicted of violation of these unlawful acts; now, therefore,

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That subheading "Fraud—Conversion by Factors of Consigned Goods" of Article 27—Crimes and Punishments of the Annotated Code of Maryland be and it is hereby redesignated to apply to Section(s) 170 through 172 only.

SECTION 2. AND BE IT FURTHER ENACTED, That section(s) of the Annotated Code of Maryland be repealed, amended, or enacted to read as follows:

Article 27—Crimes and Punishments

FRAUD—COMPUTER

169.

(A) In this subheading, the following words have the meanings indicated.

(B) "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.

(C) "Computer" means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.

(D) "Computer network" means the interconnection of communication lines with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(E) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from a computer system.

(F) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(G) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software.

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

(I) "Person" includes the state, any county, municipal corporation or other political subdivision of the state, or any of its units, or an individual, receiver, trustee, guardian, executor, administrator, fiduciary, or representative of any kind, or any partnership, firm, association, public or private corporation, or any other entity, unless otherwise provided.

(J) "Property" includes financial instruments, information, electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(K) "Services" includes computer time, data processing, and storage functions.

169A.

(A) A person may not directly or indirectly access or cause to be accessed any computer, computer system, or computer network, or any part of a computer, computer system, or computer network of another person: (1) by devising or executing any scheme or artifice to defraud, or (2) by obtaining money, financial instruments, property, or services by means of false or fraudulent pretenses, representations, or promises.

(B) A person may not intentionally without authorization, directly or indirectly gain access to, alter, damage, or destroy any computer system, or computer network described in subsection (A), or any computer software, program, or data contained in a computer, computer system, or computer network.

(C) Any person convicted under the provisions of this subheading is guilty of a felony and is subject to imprisonment for not more than 10 years or a fine of not more than $10,000, or both.

(D) A supplier of telecommunications equipment or services may operate, install, modify, alter, test, repair or disconnect telecommunications equipment or services if such act is performed:

(1) In the ordinary course of business; and

(2) Without malice.

169B.

The Provisions of this act shall be known and may be cited as the "Maryland Computer Systems Protection Act".

L-3 Massachusetts

H. 911

AN ACT RELATIVE TO THE RIGHT OF PRIVACY.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The General Laws are hereby amended by inserting after chapter 93E the following chapter:—

CHAPTER 93F.
COMPUTER PRIVACY ACT.

Section 1. For the purposes of this chapter, the following words shall, unless the context otherwise requires, have the following meanings:—

(1) "Business entity" means a sole proprietorship, partnership, corporation, association, or other group, however, organized and whether or not organized to operate at a profit. For purposes of this definition, any parent corporation and all of its subsidiaries whose outstanding voting securities are 50 percent or more owned, directly or indirectly, by the parent corporation shall be treated as a single corporation.

(2) "Agency" means any office, subdivision branch, or division of any legally constituted governmental organization in the commonwealth, except agencies of the federal government.

(3) "Individual" means a natural person and not a business entity.

(4) "Personal information" includes data which is associated with identifiable individuals, and (i) indicates things done by or to an individual, including, but not limited to, records of financial transactions, medical treatment, or other services; or (ii) affords a basis for inferring personal characteristics or things done by or to an individual, including the mere record of this presence in a place, attendance at a meeting, or admission to some type of institution. "Personal information" shall not include:

(A) Data which is acquired in the ordinary course of business transactions regarding experiences and transactions between an individual and an organization maintaining a record thereof for internal use only, such as production reporting, production scheduling, production inspection, or account verification.

(B) Data consisting only of names, addresses, telephone numbers, or occupations.

(C) Data compiled from those public records which under law impart constructive notice of matters affecting title to real property.

(5) "Data subject" means an individual on whom personal information is maintained in an automated information management system.

(6) "Record" means a collection of related items of data which is created, maintained, or used by a business entity or agency as a part of an automated information management system and which contains a data subject's name, or an identifying number, symbol, or other identifying particulars that serve to explicitly identify the data subject.

(7) "Automated information management system" means a group of computer programs created to organize, catalog, locate, store, retrieve, and maintain personal information through use of a computer or other electronic information processing device from which information is retrieved by the name of a data subject or other identifying particular assigned to the data subject or other identifying particular assigned to the data subject and includes all processing operations, from initial collection of data through all uses of the data, including outputs from the system, but not including information classified pursuant to the National Security Act of 1947.

(8) "Statistical research and reporting system" means an information system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual.

(9) "Maintaining" includes collection and maintenance.

(10) "Disclosure" means the act of divulging, revealing, or opening to view.

(11) "Disseminate" means to disclose, release, transfer, or otherwise communicate information orally, in writing, or by electronic or other means.

Section 2. Notice required of recordholders.—

(a) Every business entity or agency maintaining an automated information management system accessed within the commonwealth shall give notice of the existence and character of the automated information management system prior to January 31, 1980. Notice shall be filed with the secretary of state, and shall be a permanent public record. The secretary may establish regulations prescribing the form of the notice to implement this section, and may charge a filing fee not to exceed five dollars ($5.00) for each notice filed to defray the administrative costs incurred pursuant to this section. Any business entity or agency maintaining more than one automated information management system may file notices for each of its systems separately or the notices may be combined as a single filing, when appropriate. Where a single automated information management system is duplicated or repeated at more than one location, under the guidance of a central office, that system may be reported as a single system, specifying each location where it is operated and where records exist which contain personal information used by the system. Where the computer or other electronic information processing device used in an automated information management system is operated by a business entity or agency other than the business entity or agency which collects and uses the personal information contained in that automated information management system, the business entity or agency which collects and

uses the personal information, and not the business entity or agency which operates the computer or other electronic information processing device, shall be considered to be the business entity or agency maintaining the automated information management system. On or after January 31, 1980, any business entity or agency proposing to create an automated information management system or terminate an automated information management system or to change the type, use, or categories of users of personal information maintained in an automated information management system, shall file a notice with the secretary within 90 days after such action.

(b) Notices shall specify each of the following:

(1) The name of each automated information management system, the name and address of the business entity or agency maintaining the automated information management system and the title, address, and telephone number of the official to whom inquiries regarding each automated information management system may be addressed.

(2) The purposes of each automated information management system, including all uses made of the personal information contained therein, such as internal personnel administration, accounts receivable, or accounts payable.

(3) The categories of data subjects on whom personal information is or expected to be maintained in each automated information management system, such as employees, customers, or clients.

(4) The categories of personal information to be maintained, including financial, personal health, education, and property data.

(5) The categories of business entities, agencies, or individuals, which may routinely receive or use the personal information from each automated information management system.

(6) Whether the automated information management system or any portion thereof is exempted under section Nine (a), (d), or (e).

(c) Notwithstanding any other provisions of this title, every business entity or agency which fails to file a notice or which knowingly and intentionally files a notice that is false or incomplete shall be liable for a civil penalty not to exceed ten thousand dollars ($10,000) for each violation, which shall be assessed and recovered in a civil action brought in any court of competent jurisdiction in the name of the commonwealth by the attorney general and the entire amount of the penalty collected shall be paid into the general treasury.

Section 3. Notice required to data subject.—Except for statistical research and reporting systems, each business entity or agency maintaining an automated information management system shall disclose or display to each data subject asked by the business entity

or agency subsequent to January 1, 1980 to supply personal information for use in such automated information management system, at the time the personal information is requested, or in telephoned requests, at the next written communication with the individual:

(1) The categories of routine or usual recipients or users of the information.

(2) The purpose or purposes for which the information is intended to be used.

(3) Which statutes or regulations, if any, require disclosure of the information.

(4) Any action adverse to the data subject which may be taken by the business entity or agency as a result of the data subject's refusal to provide all or any part of the requested personal information.

Section 4. Disclosure of information.—Personal information contained in an automated information management system may be disclosed or disseminated to any business entity, agency, or individual only if the disclosure or dissemination is:

(1) To those officers, employers, employees, or agents of the business entity or agency maintaining the automated information management system who have a need for such personal information in the performance of their duties with the business entity or agency.

(2) In accordance with the purposes stated and to the categories of users noted in the most recent notice filed with the secretary of state pursuant to section two (b)(2) and (b)(5).

(3) Pursuant to a written request by, or with the prior written consent of, the data subject to whom the personal information pertains.

(4) To a recipient who has provided the business entity or agency with advance adequate written assurance that the personal information will be used solely in a statistical research or reporting system, and the personal information is transferred in a form that is not individually identifiable.

(5) To the state archives of the commonwealth as a record which has sufficient historical or other value to warrant its continued preservation by the commonwealth, or for the evaluation by the director of the state archives or his designee to determine whether the record has such value.

(6) To federal, state, or local government when that disclosure is authorized or required by law.

(7) To the public from records which by law or regulation are open to public inspection or copying.

(8) Pursuant to a showing of compelling circumstances affecting the health or safety of a data subject if, upon disclosure, notification is transmitted to the last known address of the data subject.

(9) To any person pursuant to a search warrant, subpoena, court order, or compulsory legal process where disclosure is required by law.

(10) To another business entity or agency which performs computer data-processing services for the business entity or agency maintaining the automated information management system.

(11) To law enforcement agencies when needed to investigate criminal activity.

Section 5. Access to records.—Each business entity or agency maintaining an automated information management system, the description of which is one filed with the secretary of state in accordance with section two shall:

(1) Make available in a reasonably comprehensible form to a data subject upon proper identification, a copy of any record or portion thereof maintained in an automated information management system containing personal information pertaining to the data subject. When a business entity or agency is unable to access a record by reference to name only, or when access to name only would impose an unreasonable administrative burden, it may require the individual to submit other identifying information as will facilitate access to the file.

(2) Permit the data subject to file a written notice of dispute identifying any personal information pertaining to the data subject which is believed by the data subject to be inaccurate, not timely, or incomplete, and which is contained in any automated information management system maintained by the business entity or agency. The notice of dispute shall: identify specifically the record and the personal information believed to be inaccurate, not timely, or incomplete; set forth the changes which the data subject believes to be necessary in order to make the personal information accurate, timely, or complete; and state the full name of the data subject and the address at which the data subject may be contacted. Upon receipt of a written notice of dispute, the business entity or agency shall either: (i) Correct or amend any portion of the disputed personal information which the data subject believes is not accurate, timely or complete or (ii) Promptly inform the data subject, in writing, or its refusal to correct or amend the record, in accordance with the data subject's request, the reasons for refusal, the procedures

established by the business entity or agency for the data subject to request a review of that refusal, the name and business address of the official within the business entity or agency to whom the request for review may be taken, and that any request for review shall be made within 30 days of receipt of notice of refusal to correct or amend the record. Any request for a review received by a business entity or agency which is in substantial compliance with the requirements of subsection (2) of this section shall be resolved within 30 days after receipt of the request.

(3) Permit any data subject whose request, pursuant to subsection (2)(ii) of this section, that the business entity or agency correct or amend the record of the data subject has been denied in whole or part by the reviewing official, to file with the business entity or agency within 30 days after the denial a concise written statement setting forth the reasons for disagreeing with the denial. The business entity or agency may limit the statement to not more than 100 words. Upon receipt of a written statement of disagreement from a data subject the business entity or agency shall either:

(i) Within a reasonable period after receipt of the written statement of disagreement, bring an action for declaratory judgment as to the dispute in a court of competent jurisdiction. In submitting the dispute to the court, the business entity or agency shall include in its pleadings the original notice of dispute, the initial refusal to correct or amend, the subsequent refusal to correct or amend made pursuant to subsection (2)(ii) of this section, and the written statement of disagreement. Should the court find in favor of the data subject, the business entity or agency shall be liable for all court costs and reasonable attorney's fees. Neither the data subject nor the business entity or agency may appeal the court's final determination, except upon the grounds that the court's final determination was arbitrary and capricious; or

(ii) In any disclosure, except in accordance with Section four (1), (4) or (8), containing personal information about which the data subject has filed a written statement of disagreement, occuring within a reasonable period of time after the filing of the statement under this subsection, clearly note that the personal information is disputed and, upon request of either the data subject of the recipient of the information, make available to the recipient a copy of the statement of disagreement or a clear and accurate codification or summary thereof until resolution of the disagreement. If the business entity or agency deems it appropriate, it may provide copies of a concise statement of the reasons for not making the corrections or amendments requested.

Section 6. Fees.—The business entity or agency may charge the data subject a reasonable fee, not to exceed $5.00, for making and supplying a copy of his record. This section does not apply when a statute or ordinance establishes the charge, or the manner of establishing a charge, for making a copy.

Section 7. Civil Remedies.—(a) Failure to comply with any provision of this title by a business entity or agency shall constitute an unfair information practice. Commission of an unfair information practice which results in injury to a data subject shall give rise to a civil cause of action which may be prosecuted by the injured data subject.

(b) In any suit brought pursuant to the provisions of subsection (a) of this section relating to refusal to provide a copy of personal information to a data subject:

(1) The court may enjoin the business entity or agency from withholding the personal information and order the production to the complainant of any personal information improperly withheld. In that case the court may examine the personal information in camera to determine whether the information or any portion thereof may be withheld, and the burden is on the business entity or agency to sustain its refusal.

(2) The court may assess reasonable attorney's fees and court costs. (c) In any suit brought pursuant to the provisions of subsection (a) of this section in which the court determines that the business entity or agency acted in a manner which was intentional, arbitrary, and capricious, the business entity or agency shall be liable to the complainant in an amount equal to the sum of:

(1) Treble the damages sustained by the complainant as a result of refusal or failure, but in no case less than $1,000; and

(2) The court costs and reasonable attorney's fees.

(d) An action to enforce any liability created under this section may be brought in any court of competent jurisdiction within two years from date on which the cause of action arose, except that where a business entity or agency has willfully misrepresented any personal information required under this act to be disclosed to a data subject and the information so misrepresented is material to the establishment of the business entity's or agency's liability to that data subject under this section, the action may be brought at any time within two years after the data subject discovered or should have discovered the misrepresentation.

Section 8. Criminal Penalties.—(a) Any person who intentionally attempts to obtain, obtains, or uses personal information from an automated information management system and who knowingly

is not authorized to obtain or use such information under Section Four, shall be fined not more than $5,000 or imprisoned in a county jail not more than one year, or both.

(b) Any person who knowingly and intentionally discloses personal information from an automated information management system to another who is not authorized to obtain such information under Section 4 shall be fined not more than $5,000 or imprisoned for not more than one year, or both.

Section 9. General Exemptions.—(a) the head of any agency may exempt any automated information management system under its jurisdiction from any part of this act except Section 2, if that system is maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime, or to pardon, or parole authorities, and which consists of the following:

(1) Personal information compiled for the purpose of identifying individual criminal offenders or alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status.

(2) Personal information compiled for the purpose of criminal investigation, including reports of informants and investigators, and associated with an identifiable individual.

(3) Reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

(4) Records consisting of criminal history or applicant entry information maintained by the department of the attorney general, to which an individual has the right of examination.

(b) The head of any business entity, agency, or an individual maintaining an automated information management system containing medical, psychiatric, or communicable disease control information may exempt portions of those records from Section Five if, in competent medical opinion, disclosure of the exempted portion to the data subject would be detrimental to the data subject. Competent medical opinion shall include the opinion of the physician who supplied or provided the information to the information systems. The information shall, upon written authorization, be disclosed to a physician designated by the data subject.

(c) Nothing in this act shall prohibit the disclosure of personal information to third parties for the purpose of processing a data sub-

ject's health claim, providing the purpose is stated in the most recent filing with the secretary of state.

(d) The head of any business entity or agency maintaining an automated information management system containing employee's records, accounts payable records, accounts receivable records, or records requested by the data subject to be disseminated periodically to any other business entity of agency may exempt the records from the requirements of Section Four.

(e) The head of any business entity or agency may exempt any automated information management system under its jurisdiction from Section Three, Five, and Six if the records contained therein are obtained from a document and if (1) the document is an official public record, (2) the document if filed or recorded with a public agency, and (d) the filing or recording of the document is required or authorized by specific statute of regulation.

(f) The head of any business entity or agency which maintains an automated information management system containing only data obtained from those public records open and available to inspection and review by the public and from those public records constituting constructive notice under law, where such records are used for such purposes as compiling, reporting, or insuring title to land, shall be exempt from the provisions of this act, provided the business entity or agency has complied with the filing requirement of Section Two.

(g) Except as may be required by compulsory legal process or otherwise required by law, nothing in this act shall require the disclosure or dissemination of any information either (1) compiled in reasonable anticipation or a court action or administrative proceeding or (2) transferred to any attorney by his client when such information otherwise would be protected by the attorney-client privilege.

Section 10. State archival records.—(a) Each state agency automated record, containing personal information, which is accepted by the director of state archives for storage, processing, and servicing shall, for the purposes of this act, be considered to be maintained by the state agency which deposited the record and shall be subject to the provisions of this act. The director of state archives shall not disclose that record, or any information therein, except to the agency responsible for the record pursuant to rules established by that agency which are not inconsistent with the provisions of this act.

(b) Each state agency automated record containing personal information which was transferred to the state archives as a record which has sufficient historical or other value to warrant its contin-

ued preservation by the commonwealth prior to the effective date of this act shall, for the purposes of this act, be considered to be maintained by the state archives and shall not be subject to the provisions of this act.

(c) Each state agency automated record containing personal information which is transferred to the state archives of the commonwealth as a record which has sufficient historical or other value to warrant its continued preservation by the commonwealth on or after the effective date of this act shall, for the purposes of this act, be considered to be maintained by the state archives and shall be subject to all provisions of this act except sections Five and Six.

Section 11. Miscellaneous provisions.—(a) No provisions of this act shall be construed to make confidential any record maintained by any business entity or agency which by law is not confidential, or to require disclosure of any record which by law is confidential, or exempt from disclosure, or the disclosure of which is prohibited by law, or to modify or alter in any manner the provisions controlling access to records, which are exempt from this act, or to encourage the creation of individual dossiers.

(b) In the event of a conflict between this act and disclosure requirements of the Federal Freedom of Information Act (Subchapter 2, commencing with Section 551, or Chapter 5, Part 1, Title 5, of the United States Code), or the Federal Family Educational Rights and Privacy Act of 1974 (20 U.S.C. 1232g) the provisions of such other act shall prevail.

(c) No provision of this act shall operate to suspend, diminish or supplant any provision of the state rules of civil procedure; neither shall any provision of this act be construed to operate to suspend, diminish, or supplant any provision for discovery in any administrative proceeding under the laws of this state.

L-4 Minnesota

S. 1033

A bill for an act
relating to crimes; specifying offenses relating to computers; providing penalties.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [609.861] [DEFINITIONS.] Subdivision 1. For the purposes of sections 1 to 8, the terms defined in this section have the meanings given them.

Subd. 2. "Intellectual property" means data including programs.

Subd. 3. "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.

Subd. 4. "Computer" means an internally-programmed, automatic device that performs data processing.

Subd. 5. "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

Subd. 6. "Computer system" means a set of related, connected or unconnected, computer equipment, devices, or computer software.

Subd. 7. "Computer network" means a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.

Subd. 8. "Computer system services" means providing a computer system or computer network to perform useful work.

Subd. 9. "Property" means anything of value and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

Subd. 10. "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

Subd. 11. "Access" means to approach, instruct, communicate with, store data, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network.

Sec. 2. [609.862] [OFFENSE AGAINST INTELLECTUAL PROPERTY.] Whoever intentionally and without authorization does any of the following is guilty of an offense against intellectual property and may be sentenced to imprisonment for not more than five years or to payment of a fine of not more than $1,000.

(1) Modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network; or

(2) Destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network; or

(3) Discloses or takes data, programs, or supporting documentation which is a trade secret within the meaning of Minnesota Statutes, Section 609.52, or is confidential as provided by law residing or

existing internal or external to a computer, computer system, or computer network.

Sec. 3. [609.863] [OFFENSE AGAINST INTELLECTUAL PROPERTY INVOLVING FRAUD.] Whoever commits an offense against intellectual property as specified in section 2 for either of the following purposes may be sentenced to imprisonment for not more than 15 years or to payment of a fine of not more than $15,000, or both:

(1) Devising or executing any scheme or artifice to defraud; or

(2) Obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises.

Sec. 4. [609.864] [OFFENSE AGAINST COMPUTER EQUIPMENT OR SUPPLIES.] Whoever intentionally and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network is guilty of an offense against computer equipment or supplies and may be sentenced to imprisonment for not more than one year or to payment of a fine of not more than $1,000.

Sec. 5. [609.865] [OFFENSE AGAINST COMPUTER EQUIPMENT OR SUPPLIES INVOLVING FRAUD.] Whoever commits an offense against computer equipment or supplies as specified in section 4 for either of the following purposes may be sentenced to imprisonment for not more than five years or to payment of a fine of not more than $5,000, or both:

(1) Devising or executing any scheme or artifice to defraud; or

(2) Obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises.

Sec. 6. [609.866] [AGGRAVATED OFFENSE AGAINST COMPUTER EQUIPMENT OR SUPPLIES.] Whoever intentionally and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network or destroys, injures, or damages any computer, computer system, or computer network is guilty of an aggravated offense against computer equipment or supplies and may be sentenced as follows:

(1) To imprisonment for not more than 15 years or to payment of a fine of not more than 15 years or to payment of a fine of not more than $15,000, or both if the damage to the computer equipment or supplies or to the computer, computer system, or computer network is $1,000 or greater, or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service, or

(2) To imprisonment for not more than five years or to payment

of a fine of not more than $5,000, or both if the damage to the computer equipment or supplies or to the computer, computer system, or computer network is greater than $200 but less than $1,000.

(3) In all other cases where the damage to the computer equipment or supplies or to the computer, computer system, or computer network is $200 or less, to imprisonment for not more than one year or to payment of a fine of not more than $5,000, or both:

Sec. 7. [609.867] [OFFENSE AGAINST COMPUTER USERS.] Whoever intentionally and without authorization does either of the following is guilty of an offense against computer users and may be sentenced to imprisonment for not more than five years or to payment of a fine of not more than $5,000, or both:

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

(2) Denies or causes the denial of computer system services to an authorized user of the 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.

Sec. 8. [609.868] [OFFENSE AGAINST COMPUTER USERS INVOLVING FRAUD.] Whoever commits an offense against computer users as specified in section 7 for either of the following purposes may be sentenced to imprisonment for not more than 15 years or to payment of a fine of not more than $15,000, or both:

(1) Devising or executing any scheme or artifice to defraud; or

(2) Obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises.

Sec. 9. This act is effective August 1, 1979 and applies to all crimes committed on or after that date.

L-5 Missouri

S. 711

AN ACT

Relating to certain crimes concerning computers, computer systems, computer networks and computer equipment and supplies, with penalty provisions.

Be it enacted by the General Assembly of the State of Missouri, as follows:

Section 1. For purposes of this act, unless the language or context clearly indicates a different meaning is intended, the following words or phrases mean:

(1) "Access", to approach, instruct, communicate with, store

data, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network;

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

(3) "Computer network", a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities;

(4) "Computer program", an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data;

(5) "Computer software", a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system;

(6) "Computer system", a set of related, connected or unconnected, computer equipment, devices, or computer software;

(7) "Computer system services", providing a computer system or computer network to perform useful work;

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

(9) "Intellectual property", data including programs;

(10) "Property", anything of value as defined in subdivision (10) of section 570.010, RSMo, and includes, but is not limited to financial instruments, information, including electronically produced data and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

Section 2. 1. A person commits the crime of an offense against intellectual property if he knowingly and without authorization:

(1) Modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network; or

(2) Destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network; or

(3) Discloses or takes data, programs, or supporting documentation which is confidential as provided by law, or which is a trade secret, residing or existing internal or external to a computer, computer system, or computer network.

2. Offense against intellectual property is a class D felony, unless the offense is committed for the purpose of devising or execut-

ing any scheme or artifice to defraud or to obtain any property, in which case offense against intellectual property is a class C felony.

Section 3. 1. A person commits the crime of an offense against computer equipment or supplies if he knowingly and without authorization:

(1) Modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network; or

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

(3) Destroys, injures, or damages any computer, computer system, or computer network.

2. Offense against computer equipment or supplies is a class A misdemeanor, unless:

(1) The offense is committed for the purpose of executing any scheme or artifice to defraud or obtain any property, in which case it is a class D felony; or

(2) The damage to such computer equipment or supplies or to the computer, computer equipment or supplies or to the computer, computer system, or computer network is greater than two hundred dollars but less than one thousand dollars, in which case it is a class D felony; or

(3) The damage to such computer equipment or supplies or to the computer, computer system, or computer network is one thousand dollars or greater or if there is an interruption or impairment of a governmental operation or of public communication, transportation, or supply of water, gas, electricity, or other essential public services, in which case it is a class C felony.

Section 4. 1. A person commits the crime of an offense against computer users if he knowingly and without authorization:

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

(2) Denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or in part, is owned by, under contract to, or operated for, or on behalf of, or in conjunction with another.

2. Offense against computer users is a class D felony unless the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property in which case an offense against computer users is a class C felony.

L-6 New Jersey

1. DEFINITIONS

a. Access: to instruct, communicate with, store data in, retrieve data from disclosed or otherwise make use of any resources of a computer, computer system or computer network.

b. Computer: an electronic device capable of executing a computer program, including arithmetic, logic, memory, or input/output operations, by the manipulation of electronic or magnetic impulses and includes all computer equipment connected to such a device in a system or network.

c. Computer Equipment: any equipment or devices including all input, output, processing, storage, software, or communications facilities, intended to interface with the computer.

d. Computer Network: the interconnection of communication lines (including microwave or other means of electronic communications) with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

e. Computer Program: a series of instructions or statements executable on a computer which directs the computer system in a manner to provide a desired result.

f. Computer Software: a set of computer programs, data, procedures and associated documentation concerned with the operation of a computer system.

g. Computer System: the combination of computer equipment, computer software and data bases intended to operate together as a cohesive system.

h. Data: a representation of facts or information in a formalized manner suitable for communication, interpretation or processing by a computer.

i. Data Base: a collection of data.

j. Data Processing: the execution of a sequence of operations performed upon data.

k. Terminal: a device capable of originating data for transmission or accepting data from transmision, or both.

l. Execute: to change the state of a computer in accordance with prescribed rules.

m. Financial Instrument: any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, marketable security, or any other written instrument which is transferable for value.

n. Instruction: a command which directs the computer to take a particular action.

o. Procedure: the course of action taken in the solution of a problem using a computer.

p. Property: financial instruments, information, data and computer software in either machine or human readable form and any other tangible or intangible item of value.

q. Services: include computer time and data storage functions.

2. INTRODUCTION OF FRAUDULENT RECORDS AND DATA

a. Whoever willfully, knowingly and without authority, directly or indirectly, accesses, causes to be accessed or attempts to access any computer, computer equipment, computer system or computer network for the purpose of the transfer of electrical impulses or the introduction of fraudulent data, data base, records, computer software, computer programs or other computer related information with the intent to devise or execute any scheme or artifice to defraud or deceive or for the purposes of obtaining money or property for themselves or another by means of false or fraudulent pretenses, representation or promises shall be guilty of a high misdemeanor and shall be subject to the penalties as set forth in Section 5.

3. INTENTIONAL ALTERATION OR DISCLOSURE

a. Whoever willfully, knowingly and without authorization, for the purposes of causing injury thereby, directly or indirectly, accesses, alters, damages or destroys any computer, computer equipment, computer network, computer system, computer program, data, data base or any other computer related item of value, either internal or external to the computer, tangible or intangible, shall be guilty of a high misdemeanor and shall be subject to the penalties as set forth in Section 5 if the damage exceeds the total of $200. The value of intangible property shall be determined separate from the media upon which it is recorded and shall be based upon the price which a willing purchaser would pay for the property to a willing seller.

b. Whoever willfully, knowingly and without authorization, directly or indirectly, discloses, causes to be disclosed or attempts to disclose data, data base, computer software or computer programs of a proprietary nature for other than fraudulent purposes shall be guilty of a high misdemeanor and shall be subject to the penalties as set forth in Section 5. The penalties of this section of the statute shall not apply in instances in which specific legislation on personal privacy applies.

4. UNAUTHORIZED ACCESS OF COMPUTER FACILITIES

a. Whoever willfully, knowingly and without authorization, indirectly or directly, accesses, causes to be accessed, or attempts to access any computer, computer equipment, computer system or computer network for the purpose of obtaining computer services for monetary or financial gain for themselves or another shall be guilty of a high misdemeanor and shall be subject to the penalties as set forth in Section 5.

5. PENALTIES

a. Conviction of a high misdemeanor under this chapter shall carry with it a penalty not to exceed a fine in the amount of not more than two and one half times the value of the property involved in the criminal activity or $10,000, whichever is greater, or imprisonment of not more than seven years or both.

6. CHAPTER NOT EXCLUSIVE

a. 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.

L-7 Pennsylvania

H. 1824

AN ACT

Amending Title 18 (Crimes and Offenses) of the Pennsylvania Consolidated Statutes, further providing for criminal mischief as to computers and specifically designating certain acts involving computers as crimes.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. Section 3304 of Title 18, act of November 25, 1970 (P.L. 707, No. 230), known as the Pennsylvania Consolidated Statutes, is amended to read:

§ 3304. Criminal mischief.

(a) Offense defined.—A person is guilty of criminal mischief if he:

(1) damages tangible property of another intentionally, recklessly, or by negligence in the employment of fire, explosives, or other dangerous means listed in section 3302(a) [of this title] (relating to causing or risking catastrophe);

(2) intentionally or recklessly tampers with tangible property of another so as to endanger person or property;

(3) intentionally or recklessly causes another to suffer pecuniary loss by deception or threat; or

(4) maliciously alters, deletes, damages or destroys any computer system, computer network, computer program or data.

(b) Grading.—Criminal mischief is a felony of the third degree if the actor intentionally causes pecuniary loss in excess of $5,000, or a substantial interruption or impairment of public communication, transportation, supply of water, gas or power, or other public service. It is a misdemeanor of the second degree if the actor intentionally causes pecuniary loss in excess of $1,000, or a misdemeanor of the third degree if he intentionally or recklessly causes pecuniary loss in excess of $500. Otherwise criminal mischief is a summary offense.

Section 2. Title 18 is amended by adding a section to read:

§ 3933. Computer theft.

(a) Offense defined.—A person is guilty of theft if he intentionally accesses or causes to be accessed any computer system or computer network for the purpose of devising or executing any scheme or artifice to defraud or extort, or obtaining money, property or services with false or fraudulent intent, representations, or promises.

(b) Definitions.—As used in this section the following words shall have the meanings given to them in this subsection:

"Accesses." To instruct, communicate with, store data in or retrieve data from a computer's system or computer network.

"Computer network." An interconnection of two or more computer systems.

"Computer program." An ordered set of instructions or statements, and related data that, when automatically executed in actual or modified form in a computer system, cause it to perform specified functions.

"Computer system." A machine or collection of machines, excluding pocket calculators, one or more of which contain computer programs and data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication and control.

"Data." A representation of information, knowledge, facts, concepts or instructions, which are being prepared or have been prepared in a formalized manner, and are intended for use in a computer system or computer network. Data also includes the work product of a computer system or computer network.

"Financial instrument." Includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter

of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security or any computer system representation thereof.

"Property." Includes but is not limited to, financial instruments, data, computer programs, documents associated with computer systems and computer programs, or copies thereof, whether tangible or intangible, including both human and computer system readable data and data while in transit.

"Service." Includes, but is not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data contained within a computer system or computer network.

Section 3. This act shall take effect in 60 days.

L-8 South Dakota

H. 1292

ENTITLED, An Act to provide property rights in computer programs and computer data and to provide penalties for unauthorized use or destruction.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF SOUTH DAKOTA:

Section 1. That § 43-2-2 be amended to read as follows:

43-2-2. There may be ownership of all inanimate things which are capable of appropriation or of manual delivery; of all domestic animals; of all obligations; of such products of labor or skill as the composition of an author, the good will of a business, computer programs and data, trade-marks, and signs, and of rights created or granted by statute.

Section 2. Terms used in this Act, unless the context requires otherwise, mean:

(1) "Computer," an internally programmed, general purpose digital device capable of automatically accepting data, processing data and supplying the results of the operation;

(2) "Computer system," a set of related, connected devices, including a computer and other devices, including but not limited to data input and output and storage devices, data communications links, and computer programs and data, that make the system capable of performing the special purpose data processing tasks for which it is specified;

(3) "Computer program," a series of coded instructions or statements in a form acceptable to a computer, which

causes the computer to process data in order to achieve a certain result.

Section 3. A person is guilty of unlawful use of a computer when he:

(1) Knowingly obtains the use of a computer system, or any part thereof, without the consent of the owner;

(2) Knowingly alters or destroys computer programs or data without the consent of the owner; or

(3) Knowingly obtains use of, alters or destroys a computer system, or any part thereof, as part of a deception for the purpose of obtaining money, property or services from the owner of a computer system or any third party.

Section 4. A person convicted of a violation of subsections (1) or (2) of section 3 of this Act where the value of the use, alteration of destruction is one thousand dollars or less is guilty of a Class 2 misdemeanor.

Section 5. A person convicted of a violation of subsections (1) or (2) of section 3 of this Act where the value of the use, alteration of destruction is more than one thousand dollars is guilty of a Class 1 misdemeanor.

Section 6. A person convicted of a violation of subsection (3) of section 3 of this Act where the value of the money, property or services obtained is one thousand dollars or less is guilty of a Class 1 misdemeanor.

Section 7. A person convicted of a violation of subsection (3) of section 3 of this Act where the value of the money, property or services obtained is more than one thousand dollars shall be guilty of a Class 4 felony.

Section 8. Sections 2 to 7, inclusive, of this Act shall neither enlarge nor diminish the rights of parties in civil litigation.

L-9 Tennessee

AN ACT making the unauthorized use of computer equipment illegal and to provide penalties for the violation of this Act.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF TENNESSEE:

SECTION 1. It shall be unlawful for any person to knowingly make an unauthorized use of any computer, computer related equipment, operating systems, programmed systems or computer time. Any person violating the provisions of this section shall be guilty of a misdemeanor and upon conviction thereof shall be punished by a fine of not less than five hundred dollars ($500), and, in

the discretion of the court, sentenced to not more than six (6) months in jail.

SECTION 2. It shall be unlawful to use any computer related equipment, operating systems, programmed systems, computer time or data stored on computer media with the intent of perpetrating a fraud or a theft by the use of such materials. Any person violating the provisions of this section shall be guilty of a felony and upon conviction thereof shall be subject to a fine of not less than one thousand dollars ($1000) nor more than ten thousand dollars ($10,000) and shall be confined in the state penitentiary for not less than one (1) year nor more than five (5) years.

SECTION 3. This Act shall take effect upon passage, the public welfare requiring it.