SB356

136824-1

By Senators Ward and Williams

RFD: Judiciary

First Read: 23-FEB-12

136824-1:n:02/21/2012:JMH/th LRS2012-912

SYNOPSIS: Existing law makes it a crime for a person to knowingly and willfully without authorization access or modify certain information or programs on a computer or in the computer system or network of another.

This bill would repeal the existing computer crime act and replace it with the Alabama Digital Crime Act.

This bill would make computer tampering a crime and would describe what acts constitute this crime.

This bill would make encoded data fraud a crime and would describe what acts constitute this crime.

This bill would make phishing a crime and would describe what acts constitute this crime.

This bill would make electronic harassment and cyberstalking crimes and would describe what acts constitute these crimes.

This bill would establish jurisdiction to prosecute certain computer crimes and jurisdiction of records related to the investigation of certain computer crimes.

This bill would provide for forfeiture of a computer or computer system owned by a defendant and used in the commission of a crime.

Amendment 621 of the Constitution of Alabama of 1901, now appearing as Section 111.05 of the Official Recompilation of the Constitution of Alabama of 1901, as amended, prohibits a general law whose purpose or effect would be to require a new or increased expenditure of local funds from becoming effective with regard to a local governmental entity without enactment by a 2/3 vote unless: it comes within one of a number of specified exceptions; it is approved by the affected entity; or the Legislature appropriates funds, or provides a local source of revenue, to the entity for the purpose.

The purpose or effect of this bill would be to require a new or increased expenditure of local funds within the meaning of the amendment. However, the bill does not require approval of a local governmental entity or enactment by a 2/3 vote to become effective because it comes within one of the specified exceptions contained in the amendment.

A BILL

TO BE ENTITLED

AN ACT

To provide for the crimes of computer tampering, encoded data fraud, phishing, electronic harassment, and cyberstalking; to provide for jurisdiction in the investigation and prosecution of certain computer crimes; to provide for forfeiture of certain computers used in a crime; to repeal Sections 13A-8-100, 13A-8-101, 13A-8-102, and 13A-8-103, Code of Alabama 1975; and in connection therewith would have as its purpose or effect the requirement of a new or increased expenditure of local funds within the meaning of Amendment 621 of the Constitution of Alabama of 1901, now appearing as Section 111.05 of the Official Recompilation of the Constitution of Alabama of 1901, as amended.

BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

Section 1. This act may be cited as The Alabama Digital Crime Act.

Section 2. As used in this act, the following terms shall have the following meanings:

(1) ACCESS. To gain entry to, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer system, or computer network.

(2) COMPUTER. An electronic, magnetic, optical, electrochemical, or other high speed data processing device or system that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

(3) COMPUTER NETWORK. The interconnection of two or more computers or computer systems that transmit data over communication circuits connecting them.

(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 or perform specific functions.

(5) COMPUTER SECURITY SYSTEM. The design, procedures, or other measures that the person responsible for the operation and use of a computer employs to restrict the use of the computer to particular persons or uses or that the owner or licensee of data stored or maintained by a computer in which the owner or licensee is entitled to store or maintain the data employs to restrict access to the data.

(6) COMPUTER SERVICES. The product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing, and storage functions.

(7) COMPUTER SOFTWARE. A set of instructions or statements, and related data, that when executed in actual or

modified form, cause a computer, computer system, or computer network to perform specific functions.

(8) COMPUTER SYSTEM. A set of related or interconnected computer or computer network equipment, devices and software.

(9) DATA. A representation of information, knowledge, facts, concepts, or instructions, which are prepared and are intended for use in a computer, computer system, or computer network. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit.

(10) ELECTRONIC MAIL MESSAGE. A message sent to a unique destination that consists of a unique user name or mailbox and a reference to an Internet domain, whether or not displayed, to which such message can be sent or delivered.

(11) FINANCIAL INSTRUMENT. Includes, but is not limited to, any check, cashier's check, draft, warrant, money order, certificate of deposit, negotiable instrument, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof.

(12) HARM. Partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.

(13) IDENTIFICATION DOCUMENT. Any document containing data that is issued to an individual and which that individual, and only that individual, uses alone or in conjunction with any other information for the primary purpose of establishing his or her identity or accessing his or her financial information or benefits. Identification documents specifically include, but are not limited to, the following:

a. Government issued driver's licenses or identification cards.

b. Payment cards such as credit cards, debit cards, and ATM cards.

c. Passports.

d. Health insurance or benefit cards.

e. Identification cards issued by educational institutions.

f. Identification cards for employees or contractors.

g. Benefit cards issued in conjunction with any government supported aid program.

h. Library cards issued by any public library.

(14) IDENTIFYING INFORMATION. Specific details that can be used to access a person's financial accounts, obtain identification, or to obtain goods or services, including, but not limited to:

a. Social Security number.

b. Driver's license number.

c. Bank account number.

d. Credit card or debit card number.

e. Personal identification number (PIN).

f. Automated or electronic signature.

g. Unique biometric data.

h. Account password.

(15) INTEGRATED CIRCUIT CARD. Also known as a smart card or chip card, a pocket sized, plastic card with embedded integrated circuits used for data storage or special purpose processing used to validate personal identification numbers (PINs), authorize purchases, verify account balances and store personal records. When inserted into a reader, it transfers data to and from a central computer.

(16) OWNER. An owner or lessee of a computer or a computer network, or an owner, lessee, or licensee of computer data, computer programs, or computer software.

(17) PROPERTY. Includes a financial instrument, data, databases, data while in transit, computer software, computer programs, documents associated with computer systems and computer programs, or copies whether tangible or intangible.

(18) RADIO FREQUENCY IDENTIFICATION (RFID). A technology that uses radio waves to transmit data remotely from an RFID tag, through a reader, from identification documents. It is used in contactless integrated circuit cards, also known as proximity cards.

(19) RADIO FREQUENCY IDENTIFICATION (RFID) TAGS. Also known as RFID labels, the hardware for an RFID system

that electronically stores and processes information, and receives and transmits the signal.

(20) REENCODER. An electronic device that places encoded information from the magnetic strip, integrated circuit, RFID tag of an identification document onto the magnetic strip, integrated circuit, or RFID tag of a different identification document.

(21) SCANNING DEVICE. A scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip, integrated circuit, or RFID tag of an identification document.

(22) TRAIT OR CHARACTERISTIC OF THAT PERSON. Includes, but is not limited to, age, color, creed, national origin, race, religion, marital status, sex, sexual orientation, gender identity, ancestry, political party preferences, political beliefs, socio-economic status, family status, or education.

(23) VIRUS. Means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

(24) WEB PAGE. A location that has a single uniform resource locator or other single location with respect to the Internet.

Section 3. (a) A person who acts without authority or who exceeds authorization of use commits the crime of computer tampering by knowingly or recklessly:

(1) Accessing, altering, damaging, or destroying any computer, computer system, or computer network.

(2) Altering, damaging, deleting, or destroying computer programs or data.

(3) Disclosing, using, controlling, or taking computer programs, data, or supporting documentation residing in, or existing internal or external to, a computer, computer system, or network.

(4) Directly or indirectly introducing a computer contaminator or a virus into any computer, computer system, or network.

(5) Disrupting or causing the disruption of a computer, computer system, or network services or denying or causing the denial of computer or network services to any authorized user of a computer, computer system, or network.

(6) Preventing a computer user from exiting a site, computer system, or network-connected location in order to compel the user's computer to continue communicating with, connecting to, or displaying the content of the service, site, or system.

(7) Obtaining any information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system, or network that is operated by this state, a political subdivision of this state, or a medical institution.

(8) Giving a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the consent of the person using the computer security system to restrict access to a computer, computer network, computer system, or data.

(b)(1) Except as otherwise provided in this subsection, the offense of computer tampering is a Class A misdemeanor, punishable as provided by law.

(2) If the actor's intent is to obtain a benefit, or defraud or harm another, the offense is a Class C felony, punishable as provided by law.

(3) If any violation results in a victim expenditure of greater than two thousand five hundred dollars ($2,500), or if there is an interruption or impairment of governmental operations or public communication, transportation, or supply of water, gas, or other public or utility service, then the offense is a Class B felony, punishable as provided by law.

(4) If any violation results in a victim expenditure of greater than one hundred thousand dollars ($100,000), or if the committed offense causes physical injury to any person who

is not involved in the act, then the offense is a Class A felony, punishable as provided by law.

(c) A prosecution for a violation of this section may be tried in any of the following:

(1) The county in which the victimized computer, computer system, or network is located.

(2) The county in which the computer, computer system, or network that was used in the commission of the offense is located or in which any books, records, documents, property, financial instruments, computer software, data, access devices, or instruments of the offense were used.

(3) The county in which any authorized user was denied service or in which an authorized user's service was interrupted.

(4) The county in which critical infrastructure resources were tampered with or affected.

Section 4. (a) A person commits the crime of encoded data fraud by:

(1) Knowingly and with the intent to defraud, possessing a scanning device; or knowingly and with intent to defraud, using or attempting to use a scanning device to access, read, obtain, memorize, or store, temporarily or permanently, information encoded on an identification document by means of magnetic strip, integrated circuit, or radio frequency identification tag without the permission of the authorized user or issuer of the identification document.

(2) Knowingly and with the intent to defraud, possessing a reencoder; or knowingly and with intent to defraud, using or attempting to use a reencoder to place encoded information on an identification document by means of magnetic strip, integrated circuit, or radio frequency identification tag without the permission of the authorized user or issuer of the identification document from which the information is being reencoded.

(b) Any person violating this section, upon conviction, shall be guilty of a Class C felony.

(c) Any scanning device or reencoder owned by the defendant and possessed or used in violation of this section may be seized and be destroyed as contraband by the investigating law enforcement agency by which the scanning device or reencoder was seized.

Section 5. (a) A person commits the crime of phishing if the person by means of an Internet web page, electronic mail message, or otherwise using the Internet, solicits, requests, or takes any action to induce another person to provide identifying information by representing that the person, either directly or by implication, is a business, without the authority or approval of the business.

(b) Any person violating this section, upon conviction, shall be guilty of a Class C felony. Multiple violations resulting from a single action or act shall constitute one violation for the purposes of this section.

(c) The following persons may bring an action against a person who violates or is in violation of this section:

(1) A person who is engaged in the business of providing Internet access service to the public, owns a web page, or owns a trademark, and is adversely affected by a violation of this section.

(2) An individual who is adversely affected by a violation of this section.

(d) In any criminal proceeding brought pursuant to this section, the crime shall be considered to be committed in any county in which any part of the crime took place, regardless of whether the defendant was ever actually present in that county, or in the county of residence of the person who is the subject of the identification documents or identifying information.

(e) The Attorney General, the district attorney, a designee of the district attorney, or any person aggrieved by a violation of subsection (a) may file a civil action in circuit court to enforce this section and to enjoin further violations of this section. The Attorney General, district attorney, a designee of the district attorney, or such aggrieved person may recover actual damages or twenty-five thousand dollars ($25,000), whichever is greater, for each violation of subsection (a).

(f) In a civil action under subsection (e), the court may increase the damage award to an amount equal to not

more than three times the award provided in subsection (d) if the court determines that the defendant has engaged in a pattern and practice of violating subsection (a).

(g) Proceeds from an action under subsection (e) shall first be used for payment of all proper expenses, including court costs, of the proceedings for the civil action with the remaining proceeds payable first towards the restitution of any victims, as determined by the court. Any remaining proceeds shall be awarded equally between the State General Fund and the office of the Attorney General, the office of the district attorney bringing the action, or both.

(h) An interactive computer service provider shall not be held liable or found in violation of this section for identifying, removing, or disabling access to an Internet web page or other online location that such provider believes in good faith is being used to engage in a violation of this section.

Section 6. (a) A person commits the crime of electronic harassment if, with intent to harass, annoy, or alarm any person, he or she transmits, posts, displays, or disseminates, by or through an electronic communication device, radio, computer, Internet, or other similar means, to any person, a communication, image, or information, which is based on the actual or perceived traits or characteristics of that person, which creates any of the following conditions:

(1) Places that person in reasonable fear or harm to his or her person or property.

(2) Has a substantial and detrimental effect on that person's physical or mental health.

(3) Has the effect of substantially interfering with that person's academic performance, employment, or other community activities or responsibilities.

(4) Has the effect of substantially interfering with that person's ability to participate in or benefit from any academic, professional, or community-based services, activities, or privileges.

(5) Has the effect of causing substantial embarrassment or humiliation within an academic or professional community.

(b) Any person violating this section, upon conviction, shall be guilty of a Class A misdemeanor.

Section 7. (a) A person commits the crime of cyberstalking if he or she does any of the following:

(1) Uses in electronic mail or electronic communication any words or language threatening to inflict physical injury to any person or to that person's child, sibling, spouse, dependent, or another individual living in the same household as the victim; or for the purpose of extorting money or other things of value from any person; or damage to the property of any person.

(2) Electronically mails or electronically communicates to another repeatedly, whether or not conversation ensues, for the purpose of threatening, terrifying, or harassing any person.

(3) Electronically mails or electronically communicates to another and knowingly makes any false statement concerning death, injury, illness, disfigurement, indecent conduct, or criminal conduct of the person electronically mailed or of any member of the person's family or household with the intent to threaten, terrify, or harass.

(4) Knowingly permits an electronic communication device under the person's control to be used for any purpose prohibited by this section.

(b) Except as otherwise provided in subsections (c) and (d), any person violating this section, upon conviction, shall be guilty of a Class A misdemeanor.

(c) If any of the following apply, the person is guilty of a Class C felony:

(1) The offense is in violation of a restraining order and the person has received actual notice of that restraining order or posting the message is in violation of an injunction or preliminary injunction.

(2) The offense is in violation of a condition of probation, a condition of parole, a condition of pretrial release, or a condition of release on bond pending appeal.

(3) The actor has been convicted and a credible threat is communicated to that actor's victim or witness, a family member of that victim or witness, or another individual living in the same household as that victim or witness.

(4) The person has been previously convicted of violating this section or a substantially similar law of

another state, a political subdivision of another state, or of the United States.

(d) This section does not apply to any peaceable, nonviolent, or nonthreatening activity intended to express political views or to provide lawful information to others. This section shall not be construed to impair any constitutionally protected activity, including speech, protest, or assembly.

Section 8. (a) A law enforcement officer, a prosecuting attorney, or the Attorney General may require the disclosure of stored wire or electronic communications, as well as transactional records pertaining thereto, to the extent and under the procedures and conditions provided for by the laws of the United States.

(b) A provider of electronic communication service or remote computing service shall provide the contents of, and transactional records pertaining to, wire and electronic communications in its possession or reasonably accessible thereto when a requesting law enforcement officer, a prosecuting attorney, or the Attorney General complies with the provisions for access thereto set forth by the laws of the United States.

(c) Search warrants for production of stored wire or electronic communications and transactional records pertaining thereto shall have statewide application or application as provided by the laws of the United States when issued by a

judge with jurisdiction over the criminal offense under investigation and to which such records relate.

(d) This section specifically authorizes any law enforcement official, prosecuting attorney, or the Attorney General to issue a subpoena to obtain any stored electronic records governed by 18 U.S.C. § 2703(b) et seq, and any successor statute. The subpoena shall be issued with a showing that the subpoenaed material relates to a pending investigation.

(e) Violation of this section shall be punishable as contempt.

Section 9. (a) An Alabama corporation that provides electronic communication services or remote computing services to the general public, when served with a warrant issued by another state to produce records that would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications, shall produce those records as if that warrant had been issued by an Alabama court.

(b) Violation of this section shall be punishable as contempt.

Section 10. (a) On conviction of a violation of this section, the court shall order that any computer, computer system, computer network, instrument of communication, software or data that was owned or used by the defendant and

that was used in the commission of the offense be forfeited to the State of Alabama and sold, destroyed, or otherwise properly disposed. If the defendant is a minor, it also includes the above listed property of the parent or guardian of the defendant. The manner, method, and procedure for the forfeiture and condemnation or forfeiture of such thing shall be the same as that provided by law for the confiscation or condemnation or forfeiture of automobiles, conveyances, or vehicles in which alcoholic beverages are illegally transported.

(b) When property is forfeited under this section, the court may award the property to any state, county, or municipal law enforcement agency or department who participated in the investigation or prosecution of the offense given rise to the seizure. The recipient law enforcement agency shall use such property for law enforcement purposes but, at its discretion, may transfer the tangible property to another governmental department or agency to support crime prevention. The agencies may sell that which is not required to be destroyed and which is not harmful to the public. The proceeds from a sale authorized by this act shall be used first for payment of all proper expenses of the proceedings for forfeiture and sale and the remaining proceeds from the sale shall be awarded and distributed by the court to the participating agencies to be used exclusively for law enforcement purposes.

Section 11. A person who is subject to prosecution under this section and any other law of this state may be prosecuted under either or both laws.

Section 12. Article 5, consisting of Sections 13A-8-100, 13A-8-101, 13A-8-102, and 13A-8-103 of Chapter 8 of Title 13A of, the Code of Alabama 1975, relating to computer crimes, is repealed.

Section 13. Although this bill would have as its purpose or effect the requirement of a new or increased expenditure of local funds, the bill is excluded from further requirements and application under Amendment 621, now appearing as Section 111.05 of the Official Recompilation of the Constitution of Alabama of 1901, as amended, because the bill defines a new crime or amends the definition of an existing crime.

Section 14. This act shall become effective on the first day of the third month following its passage and approval by the Governor, or its otherwise becoming law.