CRIMINAL LAW AMENDMENTS

2017 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Daniel W. Thatcher

House Sponsor: Lee B. Perry

LONG TITLE

General Description:

This bill amends criminal provisions relating to cybercrime and making a false report.

Highlighted Provisions:

This bill:

- defines terms;
- modifies the elements, penalties, and defenses for computer crime;
- makes it a crime to interrupt or interfere with critical infrastructure;
- amends and enacts reporting requirements relating to computer crime or the interruption of, or interference with, critical infrastructure;
- amends provisions relating to raising a false alarm or filing a false report;
- amends the elements of electronic communication harrassment; and
- makes technical and conforming changes.

Money Appropriated in this Bill:

None

Other Special Clauses:

None

Utah Code Sections Affected:

AMENDS:

76-6-702, as last amended by Laws of Utah 2005, Chapter 72

76-6-703, as last amended by Laws of Utah 2010, Chapter 193

76-6-705, as last amended by Laws of Utah 1993, Chapter 38

76-9-105, as last amended by Laws of Utah 2002, Chapter 166

76-9-201, as last amended by Laws of Utah 2009, Chapter 326

76-9-202, as last amended by Laws of Utah 2002, Chapter 166

Be it enacted by the Legislature of the state of Utah:

Section 1. Section **76-6-702** is amended to read:

76-6-702. Definitions.

As used in this part:

(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 with any of them.

(2) "Authorization" means having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

(3) "Computer" means any electronic device or communication facility that stores, [~~retrieves,~~] processes, [~~or~~] transmits, or facilitates the transmission of data.

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

(5) "Computer network" means:

(a) the interconnection of communication or telecommunication lines between:

(i) computers; or

(ii) computers and remote terminals; or

(b) the interconnection by wireless technology between:

(i) computers; or

(ii) computers and remote terminals.

(6) "Computer property" includes 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 copies of any of them.

(7) "Computer technology" includes:

(a) a computer;

(b) a computer network;

(c) computer hardware;

(d) a computer system;

(e) a computer program;

(f) computer services;

(g) computer software; or

(h) computer data.

[~~(7)~~] (8) "Confidential" means data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

(9) "Critical infrastructure" includes:

(a) a financial or banking system;

(b) any railroad, airline, airport, airway, highway, bridge, waterway, fixed guideway, or other transportation system intended for the transportation of persons or property;

(c) any public utility service, including a power, energy, gas, or water supply system;

(d) a sewage or water treatment system;

(e) a health care facility, as that term is defined in Section 26-21-2;

(f) an emergency fire, medical, or law enforcement response system;

(g) a public health facility or system;

(h) a food distribution system;

(i) a government computer system or network;

(j) a school; or

(k) other government facilities, operations, or services.

(10) "Denial of service attack" means an attack or intrusion that is intended to disrupt legitimate access to, or use of, a network resource, a machine, or computer technology.

[~~(12)~~] (11) "Financial instrument" includes any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, electronic fund transfer, automated clearing house transaction, credit card, or marketable security.

[~~(8)~~] (12) "Information" does not include information obtained:

(a) through use of:

(i) an electronic product identification or tracking system; or

(ii) other technology used by a retailer to identify, track, or price goods; and

(b) by a retailer through the use of equipment designed to read the electronic product identification or tracking system data located within the retailer's location.

(13) "Interactive computer service" means an information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including a service or system that provides access to the Internet or a system operated, or services offered, by a library or an educational institution.

[~~(9)~~] (14) "License or entitlement" includes:

(a) licenses, certificates, and permits granted by governments;

(b) degrees, diplomas, and grades awarded by educational institutions;

(c) military ranks, grades, decorations, and awards;

(d) membership and standing in organizations and religious institutions;

(e) certification as a peace officer;

(f) credit reports; and

(g) another record or datum upon which a person may be reasonably expected to rely in making decisions that will have a direct benefit or detriment to another.

[~~(10)~~] (15) "Security system" means a computer, computer system, network, or computer property that has some form of access control technology implemented, such as

encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.

[~~(11)~~] (16) "Services" include computer time, data manipulation, and storage functions.

(17) "Service provider" means a telecommunications carrier, cable operator, computer hardware or software provider, or a provider of information service or interactive computer service.

[~~(13)~~] (18) "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 including system control programs, application programs, or copies of any of them.

Section 2. Section **76-6-703** is amended to read:

76-6-703. Computer crimes and penalties -- Interfering with critical infrastructure.

[~~(1) A person who without authorization gains or attempts to gain access to and alters, damages, destroys, discloses, or modifies any computer, computer network, computer property, computer system, computer program, computer data or software, and thereby causes damage to another, or obtains money, property, information, or a benefit for any person without legal right, is guilty of:~~]

(1) It is unlawful for a person to:

(a) without authorization, or in excess of the person's authorization, access or attempt to access computer technology if the access or attempt to access results in:

(i) the alteration, damage, destruction, copying, transmission, discovery, or disclosure of computer technology;

(ii) interference with or interruption of:

(A) the lawful use of computer technology; or

(B) the transmission of data;

(iii) physical damage to or loss of real, personal, or commercial property;

(iv) audio, video, or other surveillance of another person; or

(v) economic loss to any person or entity;

(b) after accessing computer technology that the person is authorized to access, knowingly take or attempt to take unauthorized or unlawful action that results in:

(i) the alteration, damage, destruction, copying, transmission, discovery, or disclosure of computer technology;

(ii) interference with or interruption of:

(A) the lawful use of computer technology; or

(B) the transmission of data;

(iii) physical damage to or loss of real, personal, or commercial property;

(iv) audio, video, or other surveillance of another person; or

(v) economic loss to any person or entity; or

(c) knowingly engage in a denial of service attack.

(2) A person who violates Subsection (1) is guilty of:

(a) a class B misdemeanor when:

(i) the economic loss or other loss or damage caused or the value of the money, property, or benefit obtained or sought to be obtained is less than $500; or

(ii) the information obtained is not confidential;

(b) a class A misdemeanor when the economic loss or other loss or damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds $500 but is less than $1,500;

(c) a third degree felony when the economic loss or other loss or damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds $1,500 but is less than $5,000;

(d) a second degree felony when the economic loss or other loss or damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds $5,000; or

(e) a third degree felony when:

(i) the property or benefit obtained or sought to be obtained is a license or entitlement;

(ii) the damage is to the license or entitlement of another person; [~~or~~]

(iii) the information obtained is confidential; or

(iv) in gaining access the person breaches or breaks through a security system.

[~~(2)~~] (3) (a) [~~Except as provided in Subsection (2)(b), a~~] A person who intentionally or knowingly and without authorization gains or attempts to gain access to a computer, computer network, computer property, or computer system under circumstances not otherwise constituting an offense under this section is guilty of a class B misdemeanor.

(b) Notwithstanding Subsection [~~(2)~~] (3)(a), a retailer that uses an electronic product identification or tracking system, or other technology, to identify, track, or price goods is not guilty of a violation of Subsection [~~(2)~~] (3)(a) if the equipment designed to read the electronic product identification or tracking system data and used by the retailer to identify, track, or price goods is located within the retailer's location.

[~~(3)~~] (4) A person who uses or knowingly allows another person to use any computer, computer network, computer property, or computer system, program, or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises, or representations, is guilty of an offense based on the value of the money, property, services, or things of value, in the degree set forth in Subsection 76-10-1801(1).

[~~(4) A person who intentionally or knowingly and without authorization, interferes with or interrupts computer services to another authorized to receive the services is guilty of a class A misdemeanor.~~]

(5) A person is guilty of a third degree felony if the person intentionally or knowingly, and without lawful authorization, interferes with or interrupts critical infrastructure.

[~~(5)~~] (6) It is an affirmative defense to [~~Subsections~~] Subsection (1) [~~and~~], (2), or (3) that a person obtained access or attempted to obtain access:

(a) in response to, and for the purpose of protecting against or investigating, a prior attempted or successful breach of security of [~~a computer, computer network, computer property, computer system~~] computer technology whose security the person is authorized or entitled to protect, and the access attempted or obtained was no greater than reasonably necessary for that purpose[~~.~~]; or

(b) pursuant to a search warrant or a lawful exception to the requirement to obtain a search warrant.

(7) (a) An interactive computer service is not guilty of violating this section if a person violates this section using the interactive computer service and the interactive computer service did not knowingly assist the person to commit the violation.

(b) A service provider is not guilty of violating this section for:

(i) action taken in relation to a customer of the service provider, for a legitimate business purpose, to install software on, monitor, or interact with the customer's Internet or other network connection, service, or computer for network or computer security purposes, authentication, diagnostics, technical support, maintenance, repair, network management, updates of computer software or system firmware, or remote system management; or

(ii) action taken, including scanning and removing computer software, to detect or prevent the following:

(A) unauthorized or fraudulent use of a network, service, or computer software;

(B) illegal activity; or

(C) infringement of intellectual property rights.

Section 3. Section **76-6-705** is amended to read:

76-6-705. Reporting violations.

[~~Every person, except those to whom a statutory or common law privilege applies,~~]

(1) Each person who has reason to believe that the provisions of Section 76-6-703 are being or have been violated shall report the suspected violation to:

(a) the attorney general, or county attorney, or, if within a prosecution district, the

district attorney of the county or prosecution district in which part or all of the violations occurred[~~.~~]; or

(b) a state or local law enforcement agency.

(2) Subsection (1) does not apply to the extent that the person is prohibited from reporting by a statutory or common law privilege.

Section 4. Section **76-9-105** is amended to read:

76-9-105. Making a false alarm -- Penalties.

(1) A person is guilty of making a false alarm if he initiates or circulates a report or warning of any fire, impending bombing, or other crime or catastrophe, knowing that the report or warning is false or baseless and is likely to cause evacuation of any building, place of assembly, or facility of public transport, to cause public inconvenience or alarm or action of any sort by any official or volunteer agency organized to deal with emergencies.

(2) (a) [~~Making~~] A person is guilty of a second degree felony if the person makes a false alarm relating to a weapon of mass destruction as defined in Section 76-10-401 [~~is a second degree felony~~].

(b) A person is guilty of a third degree felony if:

(i) the person makes a false alarm alleging on ongoing act or event, or an imminent threat; and

(ii) the false alarm causes or threatens to cause bodily harm, serious bodily injury, or death to another person.

[~~(b)~~] (c) Making a false alarm other than under Subsection (2)(a) or (b) is a class B misdemeanor.

(3) In addition to any other penalty authorized by law, a court shall order any person convicted of a felony violation of this section to reimburse any federal, state, or local unit of government, or any private business, organization, individual, or entity for all expenses and losses incurred in responding to the violation, unless the court states on the record the reasons why the court finds the reimbursement would be inappropriate.

Section 5. Section **76-9-201** is amended to read:

76-9-201. Electronic communication harassment -- Definitions -- Penalties.

(1) As used in this section:

(a) "Adult" means a person 18 years of age or older.

(b) "Electronic communication" means any communication by electronic, electro-mechanical, or electro-optical communication device for the transmission and reception of audio, image, or text but does not include broadcast transmissions or similar communications that are not targeted at any specific individual.

(c) "Electronic communication device" includes a telephone, a facsimile machine, electronic mail, [~~or~~] a pager, a computer, or any other device or medium that can be used to communicate electronically.

(d) "Minor" means a person who is younger than 18 years of age.

(e) "Personal identifying information" means the same as that term is defined in Section 76-6-1102.

(2) A person is guilty of electronic communication harassment and subject to prosecution in the jurisdiction where the communication originated or was received if with intent to [~~annoy, alarm,~~] intimidate, [~~offend,~~] abuse, threaten, harass, frighten, or disrupt the electronic communications of another, the person:

(a) (i) makes repeated contact by means of electronic communications, regardless of whether [~~or not~~] a conversation ensues; or

(ii) after the recipient has requested or informed the person not to contact the recipient, and the person repeatedly or continuously:

(A) contacts the electronic communication device of the recipient; or

(B) causes an electronic communication device of the recipient to ring or to receive other notification of attempted contact by means of electronic communication;

(b) makes contact by means of electronic communication and insults, taunts, or challenges the recipient of the communication or any person at the receiving location in a

manner likely to provoke a violent or disorderly response;

(c) makes contact by means of electronic communication and threatens to inflict injury, physical harm, or damage to any person or the property of any person; [~~or~~]

(d) causes disruption, jamming, or overload of an electronic communication system through excessive message traffic or other means utilizing an electronic communication device[~~.~~]; or

(e) electronically publishes, posts, or otherwise discloses personal identifying information of another person, in a public online site or forum, without that person's permission.

(3) (a) (i) Electronic communication harassment committed against an adult is a class B misdemeanor, except under Subsection (3)(a)(ii).

(ii) A second or subsequent offense under Subsection (3)(a)(i) is a:

(A) class A misdemeanor if all prior violations of this section were committed against adults; and

(B) a third degree felony if any prior violation of this section was committed against a minor.

(b) (i) Electronic communication harassment committed against a minor is a class A misdemeanor, except under Subsection (3)(b)(ii).

(ii) A second or subsequent offense under Subsection (3)(b)(i) is a third degree felony, regardless of whether any prior violation of this section was committed against a minor or an adult.

(4) (a) Except under Subsection (4)(b), criminal prosecution under this section does not affect an individual's right to bring a civil action for damages suffered as a result of the commission of any of the offenses under this section.

(b) This section does not create any civil cause of action based on electronic communications made for legitimate business purposes.

Section 6. Section **76-9-202** is amended to read:

76-9-202. Emergency reporting -- Interference -- False report.

(1) As used in this section:

(a) "Emergency" means a situation in which property or human life is in jeopardy and the prompt summoning of aid is essential to the preservation of human life or property.

(b) "Party line" means a subscriber's line or telephone circuit [~~consisting~~]:

(i) that consists of two or more connected main telephone stations [~~connected therewith, each station with~~]; and

(ii) where each telephone station has a distinctive ring or telephone number.

(2) A person is guilty of emergency reporting abuse if [~~he~~] the person:

(a) intentionally refuses to yield or surrender the use of a party line or a public pay telephone to another person upon being informed that the telephone is needed to report a fire or summon police, medical, or other aid in case of emergency, unless the telephone is likewise being used for an emergency call;

(b) asks for or requests the use of a party line or a public pay telephone on the pretext that an emergency exists, knowing that no emergency exists; [~~or~~]

(c) reports an emergency or causes an emergency to be reported to any public, private, or volunteer entity whose purpose is to respond to fire, police, or medical emergencies, when the [~~actor~~] person knows the reported emergency does not exist[~~.~~]; or

(d) makes a false report, or intentionally aids, abets, or causes a third party to make a false report, to an emergency response service, including a law enforcement dispatcher or a 911 emergency response service, if the false report claims that:

(i) an ongoing emergency exists;

(ii) the emergency described in Subsection (2)(d)(i) currently involves, or involves an imminent threat of, serious bodily injury, serious physical injury, or death; and

(iii) the emergency described in Subsection (2)(d)(i) is occurring at a specified location.

(3) (a) A violation of Subsection (2)(a) or (b) is a class C misdemeanor.

(b) A violation of Subsection (2)(c) is a class B misdemeanor, except as provided under Subsection (3)(c).

(c) A violation of Subsection (2)(c) is a second degree felony if the report is regarding a weapon of mass destruction, as defined in Section 76-10-401.

(d) A violation of Subsection (2)(d):

(i) except as provided in Subsection (3)(d)(ii), is a third degree felony; or

(ii) is a second degree felony if, while acting in response to the report, the emergency responders cause physical injury to a person at the location described in Subsection (2)(d)(iii).

(4) (a) In addition to any other penalty authorized by law, a court shall order any person convicted of a violation of this section to reimburse:

(i) any federal, state, or local unit of government, or any private business, organization, individual, or entity for all expenses and losses incurred in responding to the violation[~~, unless~~]; and

(ii) any person described in Subsection (3)(d)(ii) for the costs for the treatment of the physical injury and any psychological injury caused by the offense.

(b) The court may order that the defendant pay less than the full amount of the costs described in Subsection (4)(a) only if the court states on the record the reasons why the reimbursement would be inappropriate.