PENAL CODE

TITLE 7. OFFENSES AGAINST PROPERTY

CHAPTER 33. COMPUTER CRIMES

Sec. 33.01. DEFINITIONS. In this chapter:

(1) "Access" means to approach, 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 network, computer program, or computer system.

(2) "Aggregate amount" means the amount of:

(A) any direct or indirect loss incurred by a victim, including the value of money, property, or service stolen, appropriated, or rendered unrecoverable by the offense; or

(B) any expenditure required by the victim to:

(i) determine whether data or a computer, computer network, computer program, or computer system was altered, acquired, appropriated, damaged, deleted, or disrupted by the offense; or

(ii) attempt to restore, recover, or replace any data altered, acquired, appropriated, damaged, deleted, or disrupted.

(3) "Communication common carrier" means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.

(4) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device 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.

(5) "Computer network" means the interconnection of two or more computers or computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.

(6) "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 or perform specific functions.

(7) "Computer services" means 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.

(8) "Computer system" means any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network.

(9) "Computer software" means a set of computer programs, procedures, and associated documentation related to the operation of a computer, computer system, or computer network.

(10) "Computer 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.

(10-a) "Critical infrastructure facility" means:

(A) a chemical manufacturing facility;

(B) a refinery;

(C) an electrical power generating facility, substation, switching station, electrical control center, or electrical transmission or distribution facility;

(D) a water intake structure, water treatment facility, wastewater treatment plant, or pump station;

(E) a natural gas transmission compressor station;

(F) a liquid natural gas terminal or storage facility;

(G) a telecommunications central switching office;

(H) a port, railroad switching yard, trucking terminal, or other freight transportation facility;

(I) a gas processing plant, including a plant used in the processing, treatment, or fractionation of natural gas;

(J) a transmission facility used by a federally licensed radio or television station; or

(K) a cable television or video service provider headend.

(11) "Data" means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, laser storage media, and punchcards, or may be stored internally in the memory of the computer.

(11-a) "Decryption," "decrypt," or "decrypted" means the decoding of encrypted communications or information, whether by use of a decryption key, by breaking an encryption formula or algorithm, or by the interference with a person's use of an encryption service in a manner that causes information or communications to be stored or transmitted without encryption.

(12) "Effective consent" includes consent by a person legally authorized to act for the owner. Consent is not effective if:

(A) induced by deception, as defined by Section 31.01, or induced by coercion;

(B) given by a person the actor knows is not legally authorized to act for the owner;

(C) given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property dispositions;

(D) given solely to detect the commission of an offense; or

(E) used for a purpose other than that for which the consent was given.

(13) "Electric utility" has the meaning assigned by Section 31.002, Utilities Code.

(13-a) "Encrypted private information" means

encrypted data, documents, wire or electronic communications, or other information stored on a computer or computer system, whether in the possession of the owner or a provider of an electronic communications service or a remote computing service, and which has not been accessible to the public.

(13-b) "Encryption," "encrypt," or "encrypted" means the encoding of data, documents, wire or electronic communications, or other information, using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized access to, such information.

(13-c) "Encryption service" means a computing service, a computer device, computer software, or technology with encryption capabilities, and includes any subsequent version of or update to an encryption service.

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

(14-a) "Identifying information" has the meaning assigned by Section 32.51.

(15) "Owner" means a person who:

(A) has title to the property, possession of the property, whether lawful or not, or a greater right to possession of the property than the actor;

(B) has the right to restrict access to the property; or

(C) is the licensee of data or computer software.

(15-a) "Privileged information" means:

(A) protected health information, as that term is defined by Section 182.002, Health and Safety Code;

(B) information that is subject to the attorney-client privilege; or

(C) information that is subject to the accountant-client privilege under Section 901.457, Occupations Code, or other law, if the information is on a computer, computer network, or computer system owned by a person possessing a license

issued under Subchapter H, Chapter 901, Occupations Code.

(16) "Property" means:

(A) tangible or intangible personal property including a computer, computer system, computer network, computer software, or data; or

(B) the use of a computer, computer system, computer network, computer software, or data.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, Sec. 1, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 306, Sec. 1, eff. Sept. 1, 1997; Acts 1999, 76th Leg., ch. 62, Sec. 18.44, eff. Sept. 1, 1999.

Amended by:

Acts 2011, 82nd Leg., R.S., Ch. 1044 (H.B. 3396), Sec. 1, eff. September 1, 2011.

Acts 2017, 85th Leg., R.S., Ch. 684 (H.B. 9), Sec. 2, eff. September 1, 2017.

Acts 2017, 85th Leg., R.S., Ch. 1058 (H.B. 2931), Sec. 3.17, eff. January 1, 2019.

Sec. 33.02. BREACH OF COMPUTER SECURITY. (a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(b) An offense under Subsection (a) is a Class B misdemeanor, except that the offense is a state jail felony if:

(1) the defendant has been previously convicted two or more times of an offense under this chapter; or

(2) the computer, computer network, or computer system is owned by the government or a critical infrastructure facility.

(b-1) A person commits an offense if, with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses:

(1) a computer, computer network, or computer system without the effective consent of the owner; or

(2) a computer, computer network, or computer system:

(A) that is owned by:

(i) the government; or

(ii) a business or other commercial entity engaged in a business activity;

(B) in violation of:

(i) a clear and conspicuous prohibition by the owner of the computer, computer network, or computer system; or

(ii) a contractual agreement to which the person has expressly agreed; and

(C) with the intent to obtain or use a file, data, or proprietary information stored in the computer, network, or system to defraud or harm another or alter, damage, or delete property.

(b-2) An offense under Subsection (b-1) is:

(1) a Class C misdemeanor if the aggregate amount involved is less than $100;

(2) a Class B misdemeanor if the aggregate amount involved is $100 or more but less than $750;

(3) a Class A misdemeanor if the aggregate amount involved is $750 or more but less than $2,500;

(4) a state jail felony if the aggregate amount involved is $2,500 or more but less than $30,000;

(5) a felony of the third degree if the aggregate amount involved is $30,000 or more but less than $150,000;

(6) a felony of the second degree if:

(A) the aggregate amount involved is $150,000 or more but less than $300,000;

(B) the aggregate amount involved is any amount less than $300,000 and the computer, computer network, or computer system is owned by the government or a critical infrastructure facility; or

(C) the actor obtains the identifying information of another by accessing only one computer, computer network, or computer system; or

(7) a felony of the first degree if:

(A) the aggregate amount involved is $300,000 or more; or

(B) the actor obtains the identifying

information of another by accessing more than one computer, computer network, or computer system.

(c) When benefits are obtained, a victim is defrauded or harmed, or property is altered, damaged, or deleted in violation of this section, whether or not in a single incident, the conduct may be considered as one offense and the value of the benefits obtained and of the losses incurred because of the fraud, harm, or alteration, damage, or deletion of property may be aggregated in determining the grade of the offense.

(d) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

(e) It is a defense to prosecution under this section that the person acted with the intent to facilitate a lawful seizure or search of, or lawful access to, a computer, computer network, or computer system for a legitimate law enforcement purpose.

(f) It is a defense to prosecution under Subsection (b-1)(2) that the actor's conduct consisted solely of action taken pursuant to a contract that was entered into with the owner of the computer, computer network, or computer system for the purpose of assessing the security of the computer, network, or system or providing other security-related services.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, Sec. 2, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 306, Sec. 2, eff. Sept. 1, 1997; Acts 2001, 77th Leg., ch. 1411, Sec. 1, eff. Sept. 1, 2001.

Amended by:

Acts 2011, 82nd Leg., R.S., Ch. 1044 (H.B. 3396), Sec. 2, eff. September 1, 2011.

Acts 2015, 84th Leg., R.S., Ch. 154 (H.B. 896), Sec. 1, eff. September 1, 2015.

Acts 2015, 84th Leg., R.S., Ch. 1251 (H.B. 1396), Sec. 23, eff. September 1, 2015.

Sec. 33.021. ONLINE SOLICITATION OF A MINOR. (a) In this section:

(1) "Minor" means:

(A) an individual who is younger than 17 years of age; or

(B) an individual whom the actor believes to be younger than 17 years of age.

(2) "Sexual contact," "sexual intercourse," and "deviate sexual intercourse" have the meanings assigned by Section 21.01.

(3) "Sexually explicit" means any communication, language, or material, including a photographic or video image, that relates to or describes sexual conduct, as defined by Section 43.25.

(b) A person who is 17 years of age or older commits an offense if, with the intent to commit an offense listed in Article 62.001(5)(A), (B), or (K), Code of Criminal Procedure, the person, over the Internet, by electronic mail or text message or other electronic message service or system, or through a commercial online service, intentionally:

(1) communicates in a sexually explicit manner with a minor; or

(2) distributes sexually explicit material to a minor.

(c) A person commits an offense if the person, over the Internet, by electronic mail or text message or other electronic message service or system, or through a commercial online service, knowingly solicits a minor to meet another person, including the actor, with the intent that the minor will engage in sexual contact, sexual intercourse, or deviate sexual intercourse with the actor or another person.

(d) It is not a defense to prosecution under Subsection (c) that the meeting did not occur.

(e) It is a defense to prosecution under this section that at the time conduct described by Subsection (c) was committed:

(1) the actor was married to the minor; or

(2) the actor was not more than three years older than the minor and the minor consented to the conduct.

(f) An offense under Subsection (b) is a felony of the third degree, except that the offense is a felony of the second degree if

the minor is younger than 14 years of age or is an individual whom the actor believes to be younger than 14 years of age at the time of the commission of the offense. An offense under Subsection (c) is a felony of the second degree.

(g) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

Added by Acts 2005, 79th Leg., Ch. 1273 (H.B. 2228), Sec. 1, eff. June 18, 2005.

Amended by:

Acts 2007, 80th Leg., R.S., Ch. 610 (H.B. 401), Sec. 2, eff. September 1, 2007.

Acts 2007, 80th Leg., R.S., Ch. 1291 (S.B. 6), Sec. 7, eff. September 1, 2007.

Acts 2015, 84th Leg., R.S., Ch. 61 (S.B. 344), Sec. 1, eff. September 1, 2015.

Acts 2015, 84th Leg., R.S., Ch. 61 (S.B. 344), Sec. 2, eff. September 1, 2015.

Sec. 33.022. ELECTRONIC ACCESS INTERFERENCE. (a) A person, other than a network provider or online service provider acting for a legitimate business purpose, commits an offense if the person intentionally interrupts or suspends access to a computer system or computer network without the effective consent of the owner.

(b) An offense under this section is a third degree felony.

(c) It is a defense to prosecution under this section that the person acted with the intent to facilitate a lawful seizure or search of, or lawful access to, a computer, computer network, or computer system for a legitimate law enforcement purpose.

Added by Acts 2017, 85th Leg., R.S., Ch. 684 (H.B. 9), Sec. 3, eff. September 1, 2017.

Sec. 33.023. ELECTRONIC DATA TAMPERING. (a) In this section, "ransomware" means a computer contaminant or lock that restricts access by an unauthorized person to a computer, computer system, or computer network or any data in a computer, computer

system, or computer network under circumstances in which a person demands money, property, or a service to remove the computer contaminant or lock, restore access to the computer, computer system, computer network, or data, or otherwise remediate the impact of the computer contaminant or lock.

(b) A person commits an offense if the person intentionally alters data as it transmits between two computers in a computer network or computer system through deception and without a legitimate business purpose.

(c) A person commits an offense if the person intentionally introduces ransomware onto a computer, computer network, or computer system through deception and without a legitimate business purpose.

(d) Subject to Subsections (d-1) and (d-2), an offense under this section is a Class C misdemeanor.

(d-1) Subject to Subsection (d-2), if it is shown on the trial of the offense that the defendant acted with the intent to defraud or harm another, an offense under this section is:

(1) a Class C misdemeanor if the aggregate amount involved is less than $100 or cannot be determined;

(2) a Class B misdemeanor if the aggregate amount involved is $100 or more but less than $750;

(3) a Class A misdemeanor if the aggregate amount involved is $750 or more but less than $2,500;

(4) a state jail felony if the aggregate amount involved is $2,500 or more but less than $30,000;

(5) a felony of the third degree if the aggregate amount involved is $30,000 or more but less than $150,000;

(6) a felony of the second degree if the aggregate amount involved is $150,000 or more but less than $300,000; and

(7) a felony of the first degree if the aggregate amount involved is $300,000 or more.

(d-2) If it is shown on the trial of the offense that the defendant knowingly restricted a victim's access to privileged information, an offense under this section is:

(1) a state jail felony if the value of the aggregate amount involved is less than $2,500;

(2) a felony of the third degree if:

(A) the value of the aggregate amount involved is $2,500 or more but less than $30,000; or

(B) a client or patient of a victim suffered harm attributable to the offense;

(3) a felony of the second degree if:

(A) the value of the aggregate amount involved is $30,000 or more but less than $150,000; or

(B) a client or patient of a victim suffered bodily injury attributable to the offense; and

(4) a felony of the first degree if:

(A) the value of the aggregate amount involved is $150,000 or more; or

(B) a client or patient of a victim suffered serious bodily injury or death attributable to the offense.

(e) When benefits are obtained, a victim is defrauded or harmed, or property is altered, appropriated, damaged, or deleted in violation of this section, whether or not in a single incident, the conduct may be considered as one offense and the value of the benefits obtained and of the losses incurred because of the fraud, harm, or alteration, appropriation, damage, or deletion of property may be aggregated in determining the grade of the offense.

(f) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

(g) Software is not ransomware for the purposes of this section if the software restricts access to data because:

(1) authentication is required to upgrade or access purchased content; or

(2) access to subscription content has been blocked for nonpayment.

Added by Acts 2017, 85th Leg., R.S., Ch. 684 (H.B. 9), Sec. 3, eff. September 1, 2017.

Sec. 33.024. UNLAWFUL DECRYPTION. (a) A person commits an offense if the person intentionally decrypts encrypted private information through deception and without a legitimate business

purpose.

(b) Subject to Subsections (b-1) and (b-2), an offense under this section is a Class C misdemeanor.

(b-1) Subject to Subsection (b-2), if it is shown on the trial of the offense that the defendant acted with the intent to defraud or harm another, an offense under this section is:

(1) a Class C misdemeanor if the value of the aggregate amount involved is less than $100 or cannot be determined;

(2) a Class B misdemeanor if the value of the aggregate amount involved is $100 or more but less than $750;

(3) a Class A misdemeanor if the value of the aggregate amount involved is $750 or more but less than $2,500;

(4) a state jail felony if the value of the aggregate amount involved is $2,500 or more but less than $30,000;

(5) a felony of the third degree if the value of the aggregate amount involved is $30,000 or more but less than $150,000;

(6) a felony of the second degree if the value of the aggregate amount involved is $150,000 or more but less than $300,000; and

(7) a felony of the first degree if the value of the aggregate amount involved is $300,000 or more.

(b-2) If it is shown on the trial of the offense that the defendant knowingly decrypted privileged information, an offense under this section is:

(1) a state jail felony if the value of the aggregate amount involved is less than $2,500;

(2) a felony of the third degree if:

(A) the value of the aggregate amount involved is $2,500 or more but less than $30,000; or

(B) a client or patient of a victim suffered harm attributable to the offense;

(3) a felony of the second degree if:

(A) the value of the aggregate amount involved is $30,000 or more but less than $150,000; or

(B) a client or patient of a victim suffered bodily injury attributable to the offense; and

(4) a felony of the first degree if:

(A) the value of the aggregate amount involved is $150,000 or more; or

(B) a client or patient of a victim suffered serious bodily injury or death attributable to the offense.

(c) It is a defense to prosecution under this section that the actor's conduct was pursuant to an agreement entered into with the owner for the purpose of:

(1) assessing or maintaining the security of the information or of a computer, computer network, or computer system; or

(2) providing other services related to security.

(d) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

Added by Acts 2017, 85th Leg., R.S., Ch. 684 (H.B. 9), Sec. 3, eff. September 1, 2017.

For text of section as amended by Acts 2017, 85th Leg., R.S., Ch. 684 (H.B. 9), Sec. 4, see other Sec. 33.03.

Sec. 33.03. DEFENSES. It is an affirmative defense to prosecution under Section 33.02 or 33.022 that the actor was an officer, employee, or agent of a communication common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communication common carrier or electric utility.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Renumbered from Penal Code Sec. 33.04 and amended by Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994.

Amended by:

Acts 2017, 85th Leg., R.S., Ch. 684 (H.B. 9), Sec. 4, eff. September 1, 2017.

Acts 2017, 85th Leg., R.S., Ch. 1058 (H.B. 2931), Sec. 3.18, eff. January 1, 2019.

Sec. 33.04. ASSISTANCE BY ATTORNEY GENERAL. The attorney general, if requested to do so by a prosecuting attorney, may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or of any other offense involving the use of a computer.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Renumbered from Penal Code Sec. 33.05 by Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994.

Sec. 33.05. TAMPERING WITH DIRECT RECORDING ELECTRONIC VOTING MACHINE. (a) In this section:

(1) "Direct recording electronic voting machine" has the meaning assigned by Section 121.003, Election Code.

(2) "Measure" has the meaning assigned by Section 1.005, Election Code.

(b) A person commits an offense if the person knowingly accesses a computer, computer network, computer program, computer software, or computer system that is a part of a voting system that uses direct recording electronic voting machines and by means of that access:

(1) prevents a person from lawfully casting a vote;

(2) changes a lawfully cast vote;

(3) prevents a lawfully cast vote from being counted; or

(4) causes a vote that was not lawfully cast to be counted.

(c) An offense under this section does not require that the votes as affected by the person's actions described by Subsection (b) actually be the votes used in the official determination of the outcome of the election.

(d) An offense under this section is a felony of the first degree.

(e) Notwithstanding Section 15.01(d), an offense under Section 15.01(a) is a felony of the third degree if the offense the actor intends to commit is an offense under this section.

(f) With the consent of the appropriate local county or

district attorney, the attorney general has concurrent jurisdiction with that consenting local prosecutor to investigate or prosecute an offense under this section.

Added by Acts 2005, 79th Leg., Ch. 470 (H.B. 56), Sec. 1, eff. September 1, 2005.

Amended by:

Acts 2009, 81st Leg., R.S., Ch. 503 (S.B. 927), Sec. 1, eff. September 1, 2009.

Sec. 33.07. ONLINE IMPERSONATION. (a) A person commits an offense if the person, without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to:

(1) create a web page on a commercial social networking site or other Internet website; or

(2) post or send one or more messages on or through a commercial social networking site or other Internet website, other than on or through an electronic mail program or message board program.

(b) A person commits an offense if the person sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person:

(1) without obtaining the other person's consent;

(2) with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and

(3) with the intent to harm or defraud any person.

(c) An offense under Subsection (a) is a felony of the third degree. An offense under Subsection (b) is a Class A misdemeanor, except that the offense is a felony of the third degree if the actor commits the offense with the intent to solicit a response by emergency personnel.

(d) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

(e) It is a defense to prosecution under this section that

the actor is any of the following entities or that the actor's conduct consisted solely of action taken as an employee of any of the following entities:

(1) a commercial social networking site;

(2) an Internet service provider;

(3) an interactive computer service, as defined by 47 U.S.C. Section 230;

(4) a telecommunications provider, as defined by Section 51.002, Utilities Code; or

(5) a video service provider or cable service provider, as defined by Section 66.002, Utilities Code.

(f) In this section:

(1) "Commercial social networking site" means any business, organization, or other similar entity operating a website that permits persons to become registered users for the purpose of establishing personal relationships with other users through direct or real-time communication with other users or the creation of web pages or profiles available to the public or to other users. The term does not include an electronic mail program or a message board program.

(2) "Identifying information" has the meaning assigned by Section 32.51.

Added by Acts 2009, 81st Leg., R.S., Ch. 911 (H.B. 2003), Sec. 1, eff. September 1, 2009.

Amended by:

Acts 2011, 82nd Leg., R.S., Ch. 282 (H.B. 1666), Sec. 1, eff. September 1, 2011.

Acts 2011, 82nd Leg., R.S., Ch. 282 (H.B. 1666), Sec. 2, eff. September 1, 2011.