

PENAL CODE

TITLE 4. INCHOATE OFFENSES

CHAPTER 16. CRIMINAL INSTRUMENTS, INTERCEPTION OF WIRE OR ORAL
COMMUNICATION, AND INSTALLATION OF TRACKING DEVICE

Sec. 16.01. UNLAWFUL USE OF CRIMINAL INSTRUMENT OR MECHANICAL SECURITY DEVICE. (a) A person commits an offense if:

(1) the person possesses a criminal instrument or mechanical security device with the intent to use the instrument or device in the commission of an offense; or

(2) with knowledge of its character and with the intent to use a criminal instrument or mechanical security device or aid or permit another to use the instrument or device in the commission of an offense, the person manufactures, adapts, sells, installs, or sets up the instrument or device.

(b) For the purpose of this section:

(1) "Criminal instrument" means anything, the possession, manufacture, or sale of which is not otherwise an offense, that is specially designed, made, or adapted for use in the commission of an offense.

(2) "Mechanical security device" means a device designed or manufactured for use by a locksmith to perform services for a customer who seeks entry to a structure, motor vehicle, or other property.

(c) An offense under Subsection (a)(1) is one category lower than the offense intended. An offense under Subsection (a)(2) is a state jail felony.

Acts 1973, 63rd Leg., p. 883, ch. 399, Sec. 1, eff. Jan. 1, 1974.
Amended by Acts 1975, 64th Leg., p. 913, ch. 342, Sec. 7, eff. Sept. 1, 1975; Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994.

Amended by:

Acts 2011, 82nd Leg., R.S., Ch. 814 (H.B. [2577](#)), Sec. 1, eff. September 1, 2011.

Sec. 16.02. UNLAWFUL INTERCEPTION, USE, OR DISCLOSURE OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS. (a) In this section:

(1) "Communication common carrier," "computer trespasser," "contents," "covert entry," "electronic communication," "intercept," "interception device," "investigative or law enforcement officer," "oral communication," "protected computer," and "wire communication" have the meanings assigned by Article 18A.001, Code of Criminal Procedure.

(2) "Immediate life-threatening situation" and "member of a law enforcement unit specially trained to respond to and deal with life-threatening situations" have the meanings assigned by Article 18A.201, Code of Criminal Procedure.

(3) "Readily accessible to the general public" means, with respect to a radio communication, a communication that is not:

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of the communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone-only paging system communication;

(E) transmitted on frequencies allocated under Part 25, Subpart D, E, or F of Part 74, or Part 94 of the rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under Part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio; or

(F) an electronic communication.

(b) A person commits an offense if the person:

(1) intentionally intercepts, endeavors to intercept, or procures another person to intercept or endeavor to intercept a wire, oral, or electronic communication;

(2) intentionally discloses or endeavors to disclose to another person the contents of a wire, oral, or electronic communication if the person knows or has reason to know the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(3) intentionally uses or endeavors to use the contents of a wire, oral, or electronic communication if the person knows or is reckless about whether the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(4) knowingly or intentionally effects a covert entry for the purpose of intercepting wire, oral, or electronic communications without court order or authorization; or

(5) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any interception device to intercept any oral communication when the device:

(A) is affixed to, or otherwise transmits a signal through a wire, cable, or other connection used in wire communications; or

(B) transmits communications by radio or interferes with the transmission of communications by radio.

(c) It is an affirmative defense to prosecution under Subsection (b) that:

(1) an operator of a switchboard or an officer, employee, or agent of a communication common carrier whose facilities are used in the transmission of a wire or electronic communication intercepts a communication or discloses or uses an intercepted communication in the normal 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 carrier of the communication, unless the interception results from the communication common carrier's use of service observing or random monitoring for purposes other than mechanical or service quality control checks;

(2) an officer, employee, or agent of a communication common carrier provides information, facilities, or technical assistance to an investigative or law enforcement officer who is authorized as provided by this section to intercept a wire, oral, or electronic communication;

(3) a person acting under color of law intercepts:

(A) a wire, oral, or electronic communication, if the person is a party to the communication or if one of the parties

to the communication has given prior consent to the interception;

(B) a wire, oral, or electronic communication, if the person is acting under the authority of Chapter 18A, Code of Criminal Procedure; or

(C) a wire or electronic communication made by a computer trespasser and transmitted to, through, or from a protected computer, if:

(i) the interception did not acquire a communication other than one transmitted to or from the computer trespasser;

(ii) the owner of the protected computer consented to the interception of the computer trespasser's communications on the protected computer; and

(iii) the actor was lawfully engaged in an ongoing criminal investigation and the actor had reasonable suspicion to believe that the contents of the computer trespasser's communications likely to be obtained would be material to the investigation;

(4) a person not acting under color of law intercepts a wire, oral, or electronic communication, if:

(A) the person is a party to the communication;
or

(B) one of the parties to the communication has given prior consent to the interception, unless the communication is intercepted for the purpose of committing an unlawful act;

(5) a person acting under color of law intercepts a wire, oral, or electronic communication if:

(A) oral or written consent for the interception is given by a magistrate before the interception;

(B) an immediate life-threatening situation exists;

(C) the person is a member of a law enforcement unit specially trained to:

(i) respond to and deal with life-threatening situations; or

(ii) install interception devices; and

(D) the interception ceases immediately on

termination of the life-threatening situation;

(6) an officer, employee, or agent of the Federal Communications Commission intercepts a communication transmitted by radio or discloses or uses an intercepted communication in the normal course of employment and in the discharge of the monitoring responsibilities exercised by the Federal Communications Commission in the enforcement of Chapter 5, Title 47, United States Code;

(7) a person intercepts or obtains access to an electronic communication that was made through an electronic communication system that is configured to permit the communication to be readily accessible to the general public;

(8) a person intercepts radio communication, other than a cordless telephone communication that is transmitted between a cordless telephone handset and a base unit, that is transmitted:

(A) by a station for the use of the general public;

(B) to ships, aircraft, vehicles, or persons in distress;

(C) by a governmental, law enforcement, civil defense, private land mobile, or public safety communications system that is readily accessible to the general public, unless the radio communication is transmitted by a law enforcement representative to or from a mobile data terminal;

(D) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(E) by a marine or aeronautical communications system;

(9) a person intercepts a wire or electronic communication the transmission of which causes harmful interference to a lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of the interference;

(10) a user of the same frequency intercepts a radio communication made through a system that uses frequencies monitored by individuals engaged in the provision or the use of the system, if

the communication is not scrambled or encrypted; or

(11) a provider of an electronic communications service records the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service towards the completion of the communication, or a user of that service from fraudulent, unlawful, or abusive use of the service.

(d) A person commits an offense if the person:

(1) intentionally manufactures, assembles, possesses, or sells an interception device knowing or having reason to know that the device is designed primarily for nonconsensual interception of wire, electronic, or oral communications and that the device or a component of the device has been or will be used for an unlawful purpose; or

(2) places in a newspaper, magazine, handbill, or other publication an advertisement of an interception device:

(A) knowing or having reason to know that the device is designed primarily for nonconsensual interception of wire, electronic, or oral communications;

(B) promoting the use of the device for the purpose of nonconsensual interception of wire, electronic, or oral communications; or

(C) knowing or having reason to know that the advertisement will promote the use of the device for the purpose of nonconsensual interception of wire, electronic, or oral communications.

(e) It is an affirmative defense to prosecution under Subsection (d) that the manufacture, assembly, possession, or sale of an interception device that is designed primarily for the purpose of nonconsensual interception of wire, electronic, or oral communication is by:

(1) a communication common carrier or a provider of wire or electronic communications service or an officer, agent, or employee of or a person under contract with a communication common carrier or service provider acting in the normal course of the provider's or carrier's business;

(2) an officer, agent, or employee of a person under

contract with, bidding on contracts with, or doing business with the United States or this state acting in the normal course of the activities of the United States or this state;

(3) a member of the Department of Public Safety who is specifically trained to install wire, oral, or electronic communications intercept equipment; or

(4) a member of a local law enforcement agency that has an established unit specifically designated to respond to and deal with life-threatening situations.

(e-1) It is a defense to prosecution under Subsection (d)(1) that the interception device is possessed by a person authorized to possess the device under Section 500.008, Government Code, or Section 242.103, Human Resources Code.

(f) An offense under this section is a felony of the second degree, unless the offense is committed under Subsection (d) or (g), in which event the offense is a state jail felony.

(g) A person commits an offense if, knowing that a government attorney or an investigative or law enforcement officer has been authorized or has applied for authorization to intercept wire, electronic, or oral communications, the person obstructs, impedes, prevents, gives notice to another of, or attempts to give notice to another of the interception.

(h) Repealed by Acts 2005, 79th Leg., Ch. 889, Sec. 1, eff. June 17, 2005.

Added by Acts 1981, 67th Leg., p. 738, ch. 275, Sec. 2, eff. Aug. 31, 1981. Amended by Acts 1983, 68th Leg., p. 4878, ch. 864, Sec. 1 to 3, eff. June 19, 1983; Acts 1989, 71st Leg., ch. 1166, Sec. 16, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 790, Sec. 16, eff. Sept. 1, 1993; Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 1051, Sec. 9, eff. Sept. 1, 1997; Acts 2001, 77th Leg., ch. 1270, Sec. 11, eff. Sept. 1, 2001; Acts 2003, 78th Leg., ch. 678, Sec. 1, eff. Sept. 1, 2003.

Amended by:

Acts 2005, 79th Leg., Ch. 889 (S.B. 1551), Sec. 1, eff. June 17, 2005.

Acts 2009, 81st Leg., R.S., Ch. 1169 (H.B. 3228), Sec. 9, eff. September 1, 2009.

Acts 2011, 82nd Leg., R.S., Ch. 85 (S.B. [653](#)), Sec. 3.023, eff. September 1, 2011.

Acts 2017, 85th Leg., R.S., Ch. 1058 (H.B. [2931](#)), Sec. 2.01, eff. January 1, 2019.

Sec. 16.03. UNLAWFUL USE OF PEN REGISTER OR TRAP AND TRACE DEVICE. (a) A person commits an offense if the person knowingly installs or uses a pen register or trap and trace device to record or decode electronic or other impulses for the purpose of identifying telephone numbers dialed or otherwise transmitted on a telephone line.

(b) In this section:

(1) "Authorized peace officer," "pen register," and "trap and trace device" have the meanings assigned by Article [18B.001](#), Code of Criminal Procedure.

(2) "Communication common carrier" has the meaning assigned by Article [18A.001](#), Code of Criminal Procedure.

(c) It is an affirmative defense to prosecution under Subsection (a) that the actor is:

(1) an officer, employee, or agent of a communication common carrier and the actor installs or uses a device or equipment to record a number dialed from or to a telephone instrument in the normal course of business of the carrier for purposes of:

(A) protecting property or services provided by the carrier; or

(B) assisting another who the actor reasonably believes to be a peace officer authorized to install or use a pen register or trap and trace device under Chapter [18B](#), Code of Criminal Procedure;

(2) an officer, employee, or agent of a lawful enterprise and the actor installs or uses a device or equipment while engaged in an activity that:

(A) is a necessary incident to the rendition of service or to the protection of property of or services provided by the enterprise; and

(B) is not made for the purpose of gathering information for a law enforcement agency or private investigative

agency, other than information related to the theft of communication or information services provided by the enterprise; or

(3) a person authorized to install or use a pen register or trap and trace device under Chapter 18B, Code of Criminal Procedure.

(d) An offense under this section is a state jail felony.
Added by Acts 1985, 69th Leg., ch. 587, Sec. 6, eff. Aug. 26, 1985.
Amended by Acts 1989, 71st Leg., ch. 958, Sec. 2, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 1051, Sec. 10, eff. Sept. 1, 1997.

Amended by:

Acts 2017, 85th Leg., R.S., Ch. 1058 (H.B. 2931), Sec. 2.02, eff. January 1, 2019.

Sec. 16.04. UNLAWFUL ACCESS TO STORED COMMUNICATIONS.

(a) In this section:

(1) "Electronic communication," "user," and "wire communication" have the meanings assigned by Article 18A.001, Code of Criminal Procedure.

(2) "Electronic storage" has the meaning assigned by Article 18B.001, Code of Criminal Procedure.

(b) A person commits an offense if the person obtains, alters, or prevents authorized access to a wire or electronic communication while the communication is in electronic storage by:

(1) intentionally obtaining access without authorization to a facility through which a wire or electronic communications service is provided; or

(2) intentionally exceeding an authorization for access to a facility through which a wire or electronic communications service is provided.

(c) Except as provided by Subsection (d), an offense under Subsection (b) is a Class A misdemeanor.

(d) If committed to obtain a benefit or to harm another, an offense is a state jail felony.

(e) It is an affirmative defense to prosecution under Subsection (b) that the conduct was authorized by:

(1) the provider of the wire or electronic communications service;

(2) the user of the wire or electronic communications service;

(3) the addressee or intended recipient of the wire or electronic communication; or

(4) Chapter 18B, Code of Criminal Procedure.

Added by Acts 1989, 71st Leg., ch. 958, Sec. 3, eff. Sept. 1, 1989.

Amended by Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 1051, Sec. 11, eff. Sept. 1, 1997.

Amended by:

Acts 2017, 85th Leg., R.S., Ch. 1058 (H.B. 2931), Sec. 2.03, eff. January 1, 2019.

Sec. 16.05. ILLEGAL DIVULGENCE OF PUBLIC COMMUNICATIONS.

(a) In this section, "electronic communications service" has the meaning assigned by Article 18A.001, Code of Criminal Procedure.

(b) A person who provides electronic communications service to the public commits an offense if the person knowingly divulges the contents of a communication to another who is not the intended recipient of the communication.

(c) It is an affirmative defense to prosecution under Subsection (b) that the actor divulged the contents of the communication:

(1) as authorized by federal or state law;

(2) to a person employed, authorized, or whose facilities are used to forward the communication to the communication's destination; or

(3) to a law enforcement agency if the contents reasonably appear to pertain to the commission of a crime.

(d) Except as provided by Subsection (e), an offense under Subsection (b) that involves a scrambled or encrypted radio communication is a state jail felony.

(e) If committed for a tortious or illegal purpose or to gain a benefit, an offense under Subsection (b) that involves a radio communication that is not scrambled or encrypted:

(1) is a Class A misdemeanor if the communication is

not a public land mobile radio service communication or a paging service communication; or

(2) is a Class C misdemeanor if the communication is a public land mobile radio service communication or a paging service communication.

(f) Repealed by Acts 1997, 75th Leg., ch. 1051, Sec. 13, eff. Sept. 1, 1997.

Added by Acts 1989, 71st Leg., ch. 1166, Sec. 17, eff. Sept. 1, 1989. Renumbered from Penal Code Sec. 16.04 by Acts 1990, 71st Leg., 6th C.S., ch. 12, Sec. 2(24), eff. Sept. 6, 1990. Amended by Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 1051, Sec. 12, 13, eff. Sept. 1, 1997.

Amended by:

Acts 2017, 85th Leg., R.S., Ch. 1058 (H.B. [2931](#)), Sec. 2.04, eff. January 1, 2019.

Sec. 16.06. UNLAWFUL INSTALLATION OF TRACKING DEVICE. (a)
In this section:

(1) "Electronic or mechanical tracking device" means a device capable of emitting an electronic frequency or other signal that may be used by a person to identify, monitor, or record the location of another person or object.

(2) "Motor vehicle" has the meaning assigned by Section [501.002](#), Transportation Code.

(b) A person commits an offense if the person knowingly installs an electronic or mechanical tracking device on a motor vehicle owned or leased by another person.

(c) An offense under this section is a Class A misdemeanor.

(d) It is an affirmative defense to prosecution under this section that the person:

(1) obtained the effective consent of the owner or lessee of the motor vehicle before the electronic or mechanical tracking device was installed;

(2) assisted another whom the person reasonably believed to be a peace officer authorized to install the device in the course of a criminal investigation or pursuant to an order of a court to gather information for a law enforcement agency; or

(3) was a private investigator licensed under Chapter [1702](#), Occupations Code, who installed the device:

(A) with written consent:

(i) to install the device given by the owner or lessee of the motor vehicle; and

(ii) to enter private residential property, if that entry was necessary to install the device, given by the owner or lessee of the property; or

(B) pursuant to an order of or other authorization from a court to gather information.

(e) This section does not apply to a peace officer who installed the device in the course of a criminal investigation or pursuant to an order of a court to gather information for a law enforcement agency.

Added by Acts 1999, 76th Leg., ch. 728, Sec. 1, eff. Sept. 1, 1999.

Amended by Acts 2001, 77th Leg., ch. 1420, Sec. 14.828, eff. Sept. 1, 2001.

Amended by:

Acts 2009, 81st Leg., R.S., Ch. 1122 (H.B. [1659](#)), Sec. 1, eff. September 1, 2009.